

# Technical Information Gathering with Maltego CE

---



**Ricardo Reimao**  
CYBER SECURITY CONSULTANT



# Automating Information Gathering

- Gather subdomains
- Gather DNS data
- Gather IP addresses
- Gather technology information
- Identify people information
- Identify email addresses
- etc.







Paterva Software



**Maltego** is an open source intelligence (OSINT) and graphical link analysis tool for gathering and connecting information for investigative tasks.





Community Edition (CE) version - FREE  
<https://www.maltego.com/>

One of the most used tools for OSINT investigations

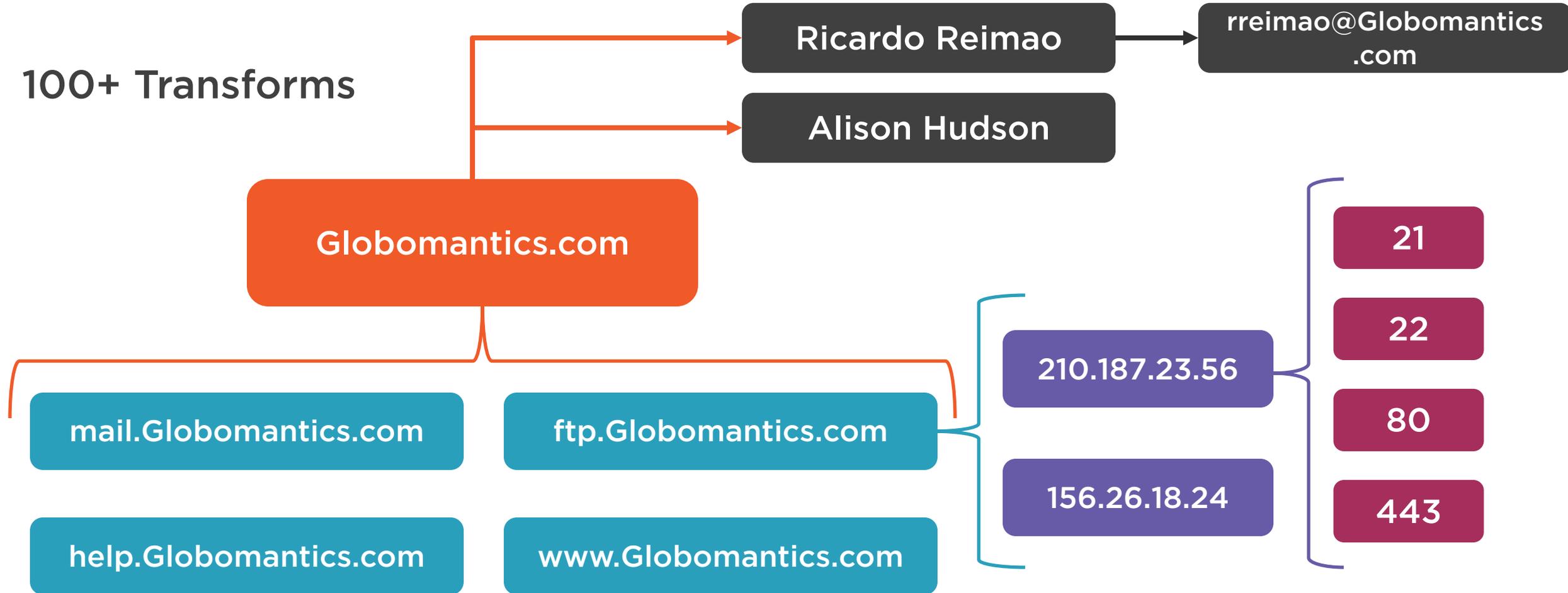
Used by large companies as well as government agencies

It is powered by the Maltego Transforms

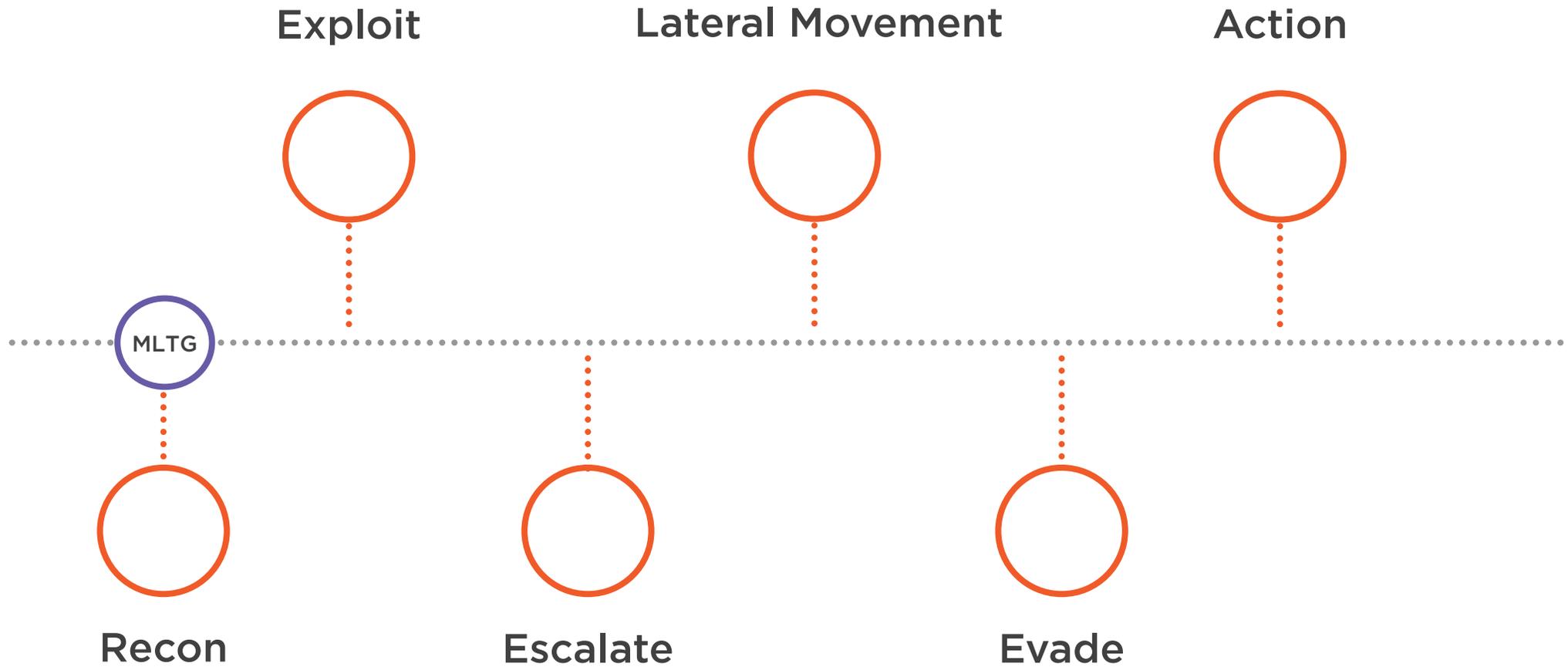


# Maltego Transforms

100+ Transforms



# Kill Chain



# MITRE PRE-ATT&CK

## Tactics

- Priority Definition Planning
- Priority Definition Direction
- Target Selection
- Technical Information Gathering
- People Information Gathering
- Organizational Information Gathering
- Technical Weakness Identification
- People Weakness Identification
- Organization Weakness Identification
- Adversary Opsec
- Establish and Maintain Infrastructure
- Persona Development
- Build Capabilities
- Test Capabilities
- Stage Capabilities



# MITRE PRE-ATT&CK

## Tactics

Priority Definition Planning

Priority Definition Direction

Target Selection

**Technical Information Gathering**

**People Information Gathering**

Organizational Information Gathering

Technical Weakness Identification

People Weakness Identification

Organization Weakness Identification

Adversary Opsec

Establish and Maintain Infrastructure

Persona Development

Build Capabilities

Test Capabilities

Stage Capabilities

T1253:

Conduct passive scanning

T1250:

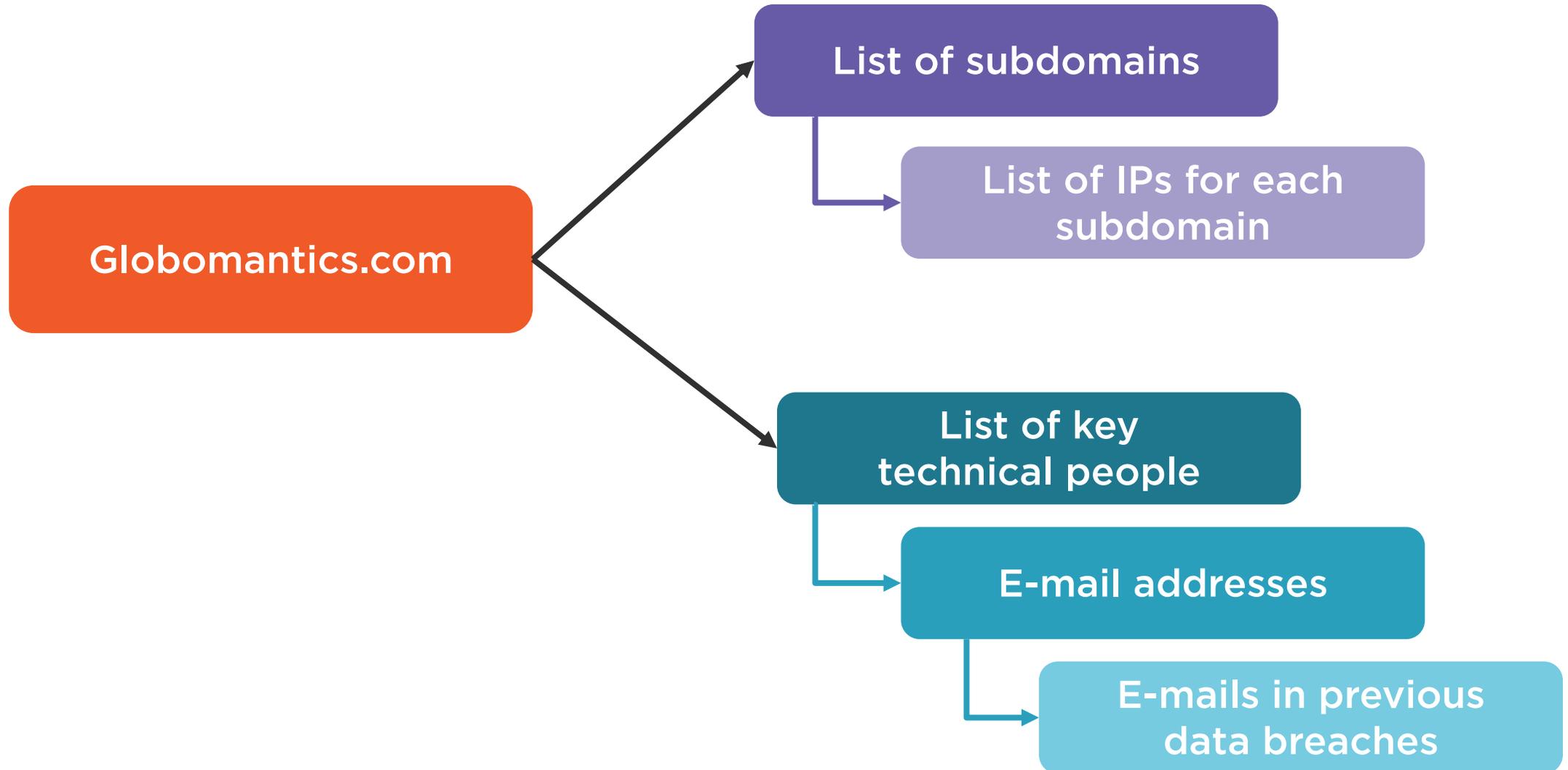
Determine domain and IP address space

T1269:

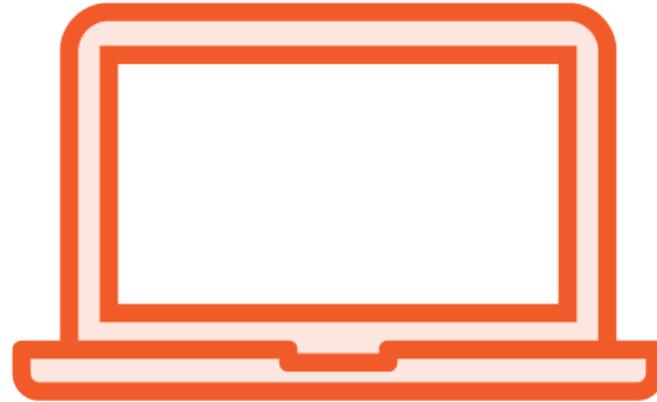
Identify People of Interest



# Attack Explanation



# Prerequisites



## **Attacker Machine**

Windows 10 or  
Kali Linux or  
MacOS



# Demo Place Holder

1. Installation Tips and Tricks
2. First use instructions and common usage syntax
3. Use of main features on live targets or in live environment



# Maltego Versions

## Community Edition

Limited transforms

Maximum 12 results  
per transform

Not for  
commercial use

## Classic/XL

All OSINT transforms

Access to  
commercial hub

Commercial Use

## Enterprise

On-premise  
deployments

Integration with  
own data

No rates or limits for  
own transforms



# Other Interesting Transforms

**Blockchain  
investigations**

**File hash  
investigations**

**Threat intelligence  
searches**

**Phone number  
lookup**

**Personal data  
enrichment**

**Shodan  
searches**

**100+ Transforms**



# More Information

## Official Documentation

Several other capabilities  
<https://www.maltego.com/>

## Professional Versions

If using for commercial purposes  
consider using Maltego XL or  
Maltego Enterprise

## Technical Information Gathering

“Technical Information Gathering  
with TheHarvester”

## Remediation

Audit your own company

Ensure personal information is not  
available to the public

Security awareness training



# Thank you!



**Ricardo Reimao**  
Cyber security consultant

