




Threat Modeling, Landscaping & Profiling

Known known, known unknowns,
and unknown unknowns



Know your Enemy!

If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.

- Sun Tzu





Know Yourself

- CIS #1 & 2
 - Tech & Hardware stack
- Digital Footprint
 - Domains
 - IPs
 - Login pages
 - Cloud providers
- Vendors
 - Software
 - Services
 - Law office
- VIPs
- Industry Peers
- Geolocation of assets.
-



What's your Secret Sauce?



- What is most valuable to your organization and where does it live?
 - Code
 - Data
 - Brand
 - Operational uptime
- What would be the most valuable to a malicious actor.
 - Customer data
 - Intellectual property
 - Operational Downtime
 - Making a Statement
 - LoLz

Ask different stakeholders



- Branch out of security
- Up and low

You will never have Whole Enchilada

- Do the best you can
- Document improvements
- Set a review period
- Verify older data



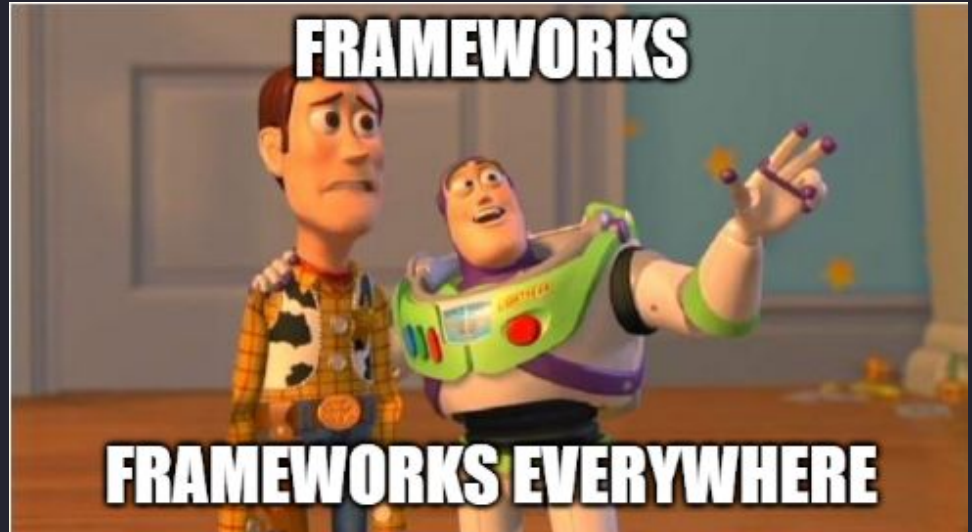
Modeling, Landscaping, and Profiling

- Looking at you
- Looking out there
- Looking at them



Threat Modeling

A risk assessment that models organizational strengths and weaknesses



Threat landscaping



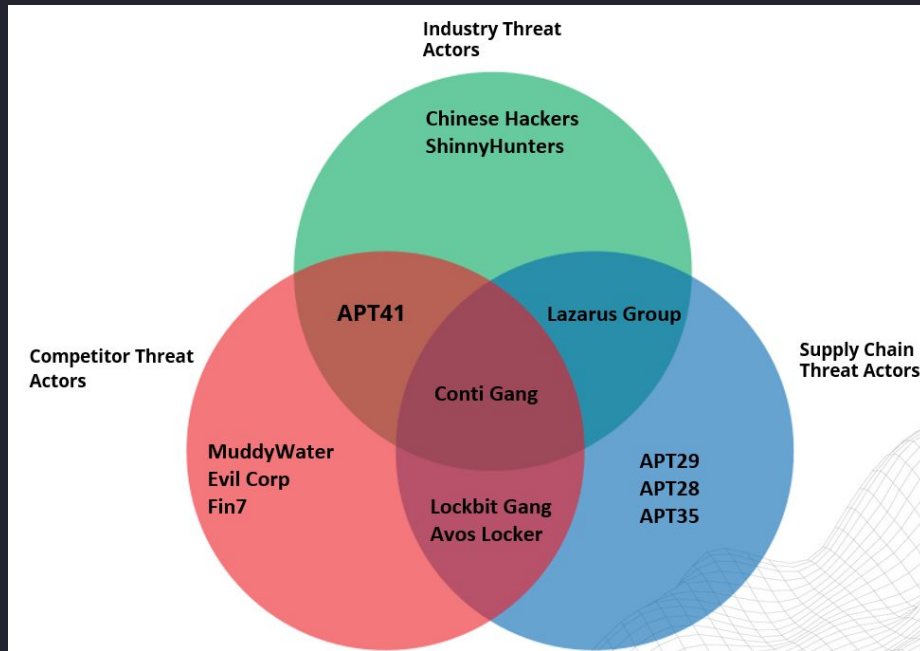
- Looking out into space to figure out what is going on out there.
 - What's hot right now?

Threat actor Profiling

Who is attacking your sector

Who is attacking your rivals

Who is might attack you for your customers



Intent and Capabilities

Actor	Alias	Intent	Capability	Category	Lists
LockBit Gang	BITWISE SPIDER	3	3.5	Financially Motivated, Ransomware group	Comp, ,SC
AvosLocker Ransomware Group		3	3.5	Financially Motivated, Ransomware group	Comp, ,SC
MuddyWater	(Cobalt Ulster, M	1	4	Nation State, Iran	Comp,
APT41	(Axiom Group, B	1	4	Nation State, China	Comp, , Industry
Conti Gang		3	3.5	Financially Motivated, Ransomware group, Easter European	Comp, , Industry, SC
Evil Corp	(Dridex Gang, G	3	3.5	Financially Motivated, Russian	Comp,
FIN7	(Carbanak)	3	4	Financially Motivated, State sponsored	Comp,
Chinese Hackers		2	3	Nation State, IP Motivated, industrial information	Industry
Lazarus Group	(HIDDEN COBRA	1	4.5	Nation State, North Korea, Financially Motivated,	Industry, SC
ShinyHunters		2	3	Financially Motivated, Underground Forum, IP and PII theft	Industry
APT29 The Dukes	(Cozer, Cozy Bea	1	4.5	Nation State, Russia, PII	SC
APT28	(Fancy Bear, Iron	1	4.5	Nation State, Russia, espionage	SC
APT35	(Group 83, News	1	4.5	Nation State, Iran,	SC











Security Analyst

**Security Operations
Manager**

CTI Analyst

Example: JAWS

Mayor understand that Amity Island weakness is loss of tourism(modeling)

Hooper to understand sharks as well as watching the coast line(Landscape)

Brody, Hooper, and Quint sent to neutralize the threat, but underestimate it(Profiling)