Numbers Game

The Case for Quantifying Cyber Threats

Scott Small, Director of Cyber Threat Intelligence

TIDAL

THREAT-INFORMED DEFENSE

whoami

Cyber Threat Intelligence Director @ Tidal Cyber (Threat-Informed Defense SaaS)

Career in intelligence research & analysis

Early work in physical security

- Importance of “actionable” intel (tuning defenses to the “local” threat landscape)

Quantifying complex security topics

	Theft	Tampering	Smuggling	Disruption	Reputation	Reputation
Country A						
Country B						
Country C						
Country D						
Country E						
Country F						

Realities of Today's Landscape

Growing Landscape: By the Numbers

Mandiant (2023): 3,500 threat groups (+900)

Microsoft (2023): 300 actors (160 nation-state, 50 ransomware)

Google TAG (2021): 270 state-sponsored groups (50 countries)

Tidal Cyber (2024): 98 ransom groups with extortion sites (+78% since '22)

ATT&CK (2023): 600+ (Sub-) Techniques

Fact: Landscape is growing – more threats are identified each year

Fact: CTI resources are limited – no team can track & address every threat at all times

Prioritization is a **must**

- But there is little consensus on how to prioritize (rank order) amongst complex threats
- A methodology for structured prioritization is needed

TIDAL

Comparing Complex Threats

≠

https://www.crowdstrike.jp/adversaries/wizard-spider/

TIDAL

Comparing Complex Threats

Tools

Intent

Proximity

Likelihood

TTPs

Sophistication

Capability

Impact

Resources

Opportunity

TIDAL

Case Study from the Physical Realm

Ongoing cargo security program launched in 2001

Overwhelming shipment volumes = unacceptable exposure

Prioritization of security validations based on **structured "risk assessments"**

- Incentives for cooperating partners

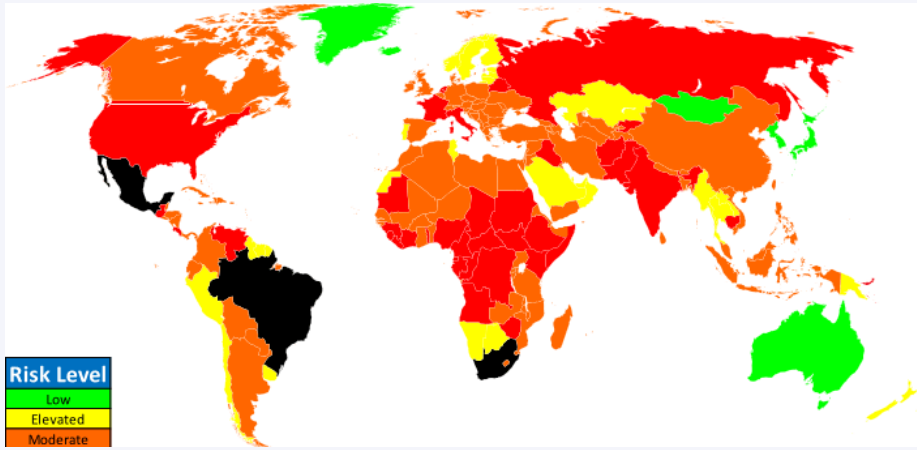
Step 2: Structured Threat Assessment

- 5 key threat areas, 3-point rating scale, **~190 countries**

C-TPAT Customs-Trade Partnership Against Terrorism

C-TPAT Risk Assessment Guide

Location: Country XYZ			
Region: Region JK	Overall Threat Rating High		
Threat Risk Factor	**Risk Rating**	**Activity**	**Source**
Terrorism (Political, Bio, Agro, Cyber)	3	2019, 2020—Recent domestic bombings and violence against U.S. based interests	Name of news publication, government site, open source information, Intel service, etc.
Contraband Smuggling	3	2019, to present— location known for narcotics exports and weapons smuggling	Name of news publication, government site, open-source information, Intel service, etc.
Human Smuggling	1	2000 to 2018— numerous incidents of human smuggling; none since 2018	Name of news publication, government site, open-source information, Intel service, etc.



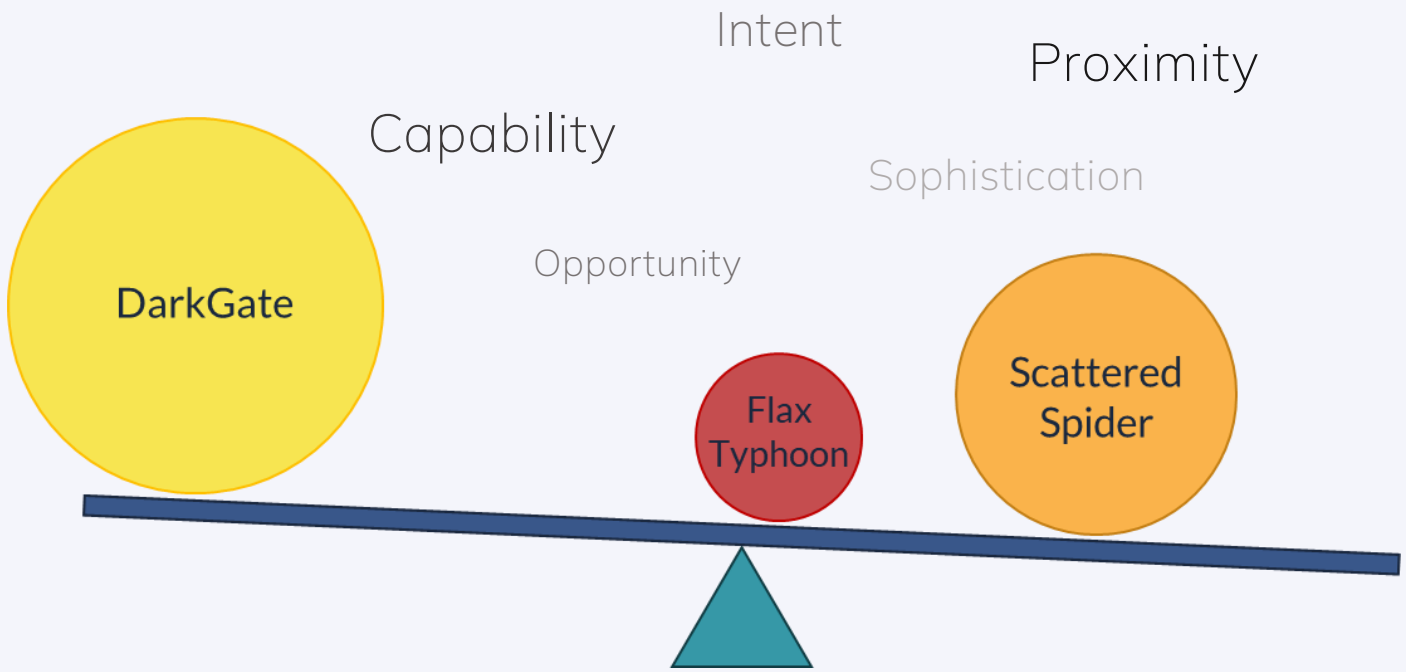
TIDAL

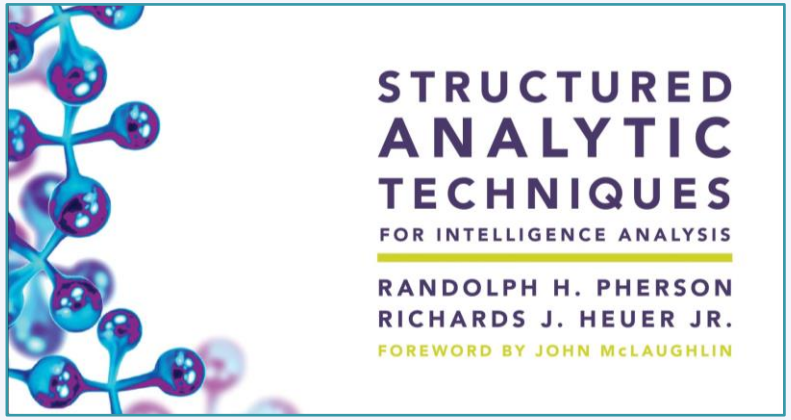
Prioritization via “Quantification”

“Threats” is an extremely complex topic…

Threat information must be **normalized** in order to make **fair** comparisons

- Check assumptions, limit bias
- Consistency
- Repeatability





“SAT for Tactical Intel”

TIDAL

Decomposing “Threat”: Quantification Criteria

- Threat
  - Intent
  - Capability / Sophistication / Capacity
  - Opportunity

TIDAL

Decomposing “Threat”: Quantification Criteria

- Threat
  - Intent
    - Proximity
      - Direct, Proximate (Industry/Peers), Indiscriminate
    - Prevalence
      - Volume, Recency, Victimology, Relationships, Reporting Attention
  - Capability / Sophistication / Capacity
    - Resources
      - State-backing? Exploits?
    - Tools
      - Type, Number/Variety, Availability
    - TTPs
      - Technique Importance

TIDAL

Popular Sources for “Normalized” CTI Data

“Intent” / “Proximity”

ETDA/ThaiCERT: Threat Encyclopedia

AlienVault OTX

MISP Threat Actor Galaxy

SecureWorks Cyber Threat Group Profiles

Palo Alto Unit42 Playbooks

CrowdStrike Threat Landscape

APT Groups & Operations (public Google Sheet)

“Capability” / “Capacity”

MITRE ATT&CK®

Ransomware victim claims (Ransomwatch/look/.live)

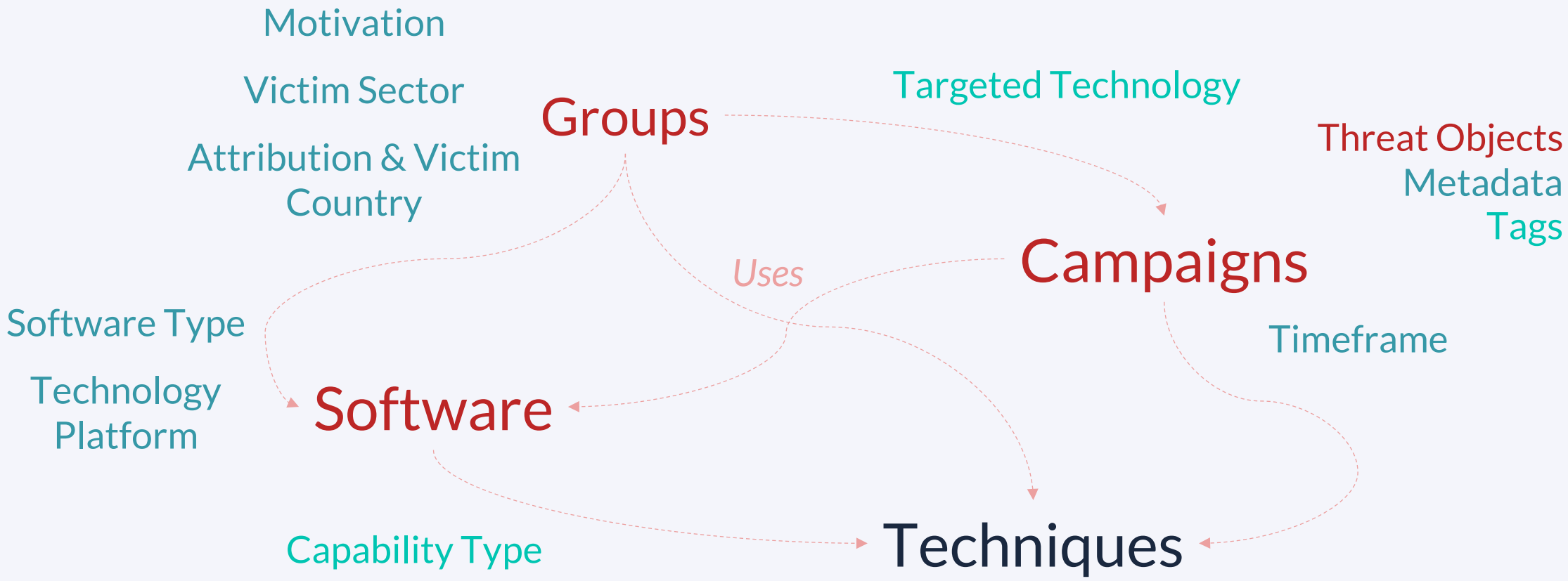
Malware sandbox trends (MalwareBazaar, Any.Run, etc)

Red Canary Intelligence Insights

Email security trends (e.g. Hornet Security Monthly Threat Roundup)

TIDAL

ATT&CK Elements + Extensions



TIDAL

Weighting	Level	Criteria	Representative Examples
5	Superior	Characterized by groups suspected of possessing near-unlimited or very large supplies of resources. Groups often consist of many operators who generally possess high levels of skill and OPSEC. Funding is typically high and provided by a state, but may be supplemented with illicit sources. Often uses custom, sophisticated tooling (alongside existing tools) and has usually been associated with multiple novel techniques or exploits.	The most advanced/prolific APTs (e.g. APT28, Lazaurs Group)
4	High	Characterized by groups suspected of possessing very large resource supplies. Group members generally possess high levels of skill and OPSEC. Funding is relatively high and may be provided by a state or illicit sources. May use custom, sophisticated tooling alongside existing tools, and might be known to periodically use novel techniques or exploits.	-Major/well-known APTs supporting major adversarial nations (e.g. APT41, Fox Kitten) -The most advanced/prolific ransomware-as-a-service operations (e.g. LockBit, ALPHV/BlackCat)
3	Moderate	Characterized by possessing access to many resources, including funding which may come from a nation-state or illicit means. These groups may be linked to a considerable volume of attacks but may also have mixed levels of success and/or periodic OPSEC blunders. May use custom tooling, but it typically does not display extreme sophistication. (This is also a common assignment for APTs and major crimeware operations when knowledge gaps remain.)	-Many APTs -Many prolific initial access threats (e.g. QakBot, SocGholish, Emotet)
1-2	Low/Limited	May be individual actors or groups, generally smaller and/or loosely organized ones. Adversaries here may claim or threaten attacks often but do not consistently follow through, at least successfully. Funding is usually limited and not at nation-state scale. Operators and their tools are usually not highly sophisticated, although some successful attacks may have occurred. Custom tools and novel exploits are uncommon. This is also a common assignment when significant knowledge gaps remain.	-Hacktivists -Lower-tier APTs & ransomware groups (including where knowledge is limited) -Infostealer campaigns

TIDAL

https://www.tidalcyber.com/threatpebookasset *(ungated)*

Methodology in Practice

Threat = Intent x Capability x Opportunity

Most practical for quantifying

Threat Profile Inputs	Intent (Proximity) Score	Capacity (Capability) Score	Final Score (Average)
APT28	5		
Andariel	5		
TA1337	5		
Wicked Panda	4		
BlackCat	3		
BumbleBee	2		
Raccoon Stealer	1		
	...		

TIDAL

Methodology in Practice

Threat = Intent x Capability x Opportunity

Most practical for quantifying

Threat Profile Inputs	Intent (Proximity) Score	Capacity (Capability) Score	Final Score (Average)*
APT28	5	5	5
Andariel	5	4	4.5
BlackCat	3	5	4*
Wicked Panda	4	4	4
TA1337	5	2	3.5
BumbleBee	2	3	2.5
Raccoon Stealer	1	2	1.5
...			

*Leave room for expert analyst judgement!

TIDAL

Pro Tips / Wrapping Up

Best Practices

- Weighting guidance
  - Leave room for expert analyst judgement
  - 1-5 is common, but narrower (and much wider) approaches exist
  - It’s ok to assign low scores!
- Recency advice
- Profile update cadence

Common Criticisms

- Aren’t most threats ultimately “the same”?

TIDAL