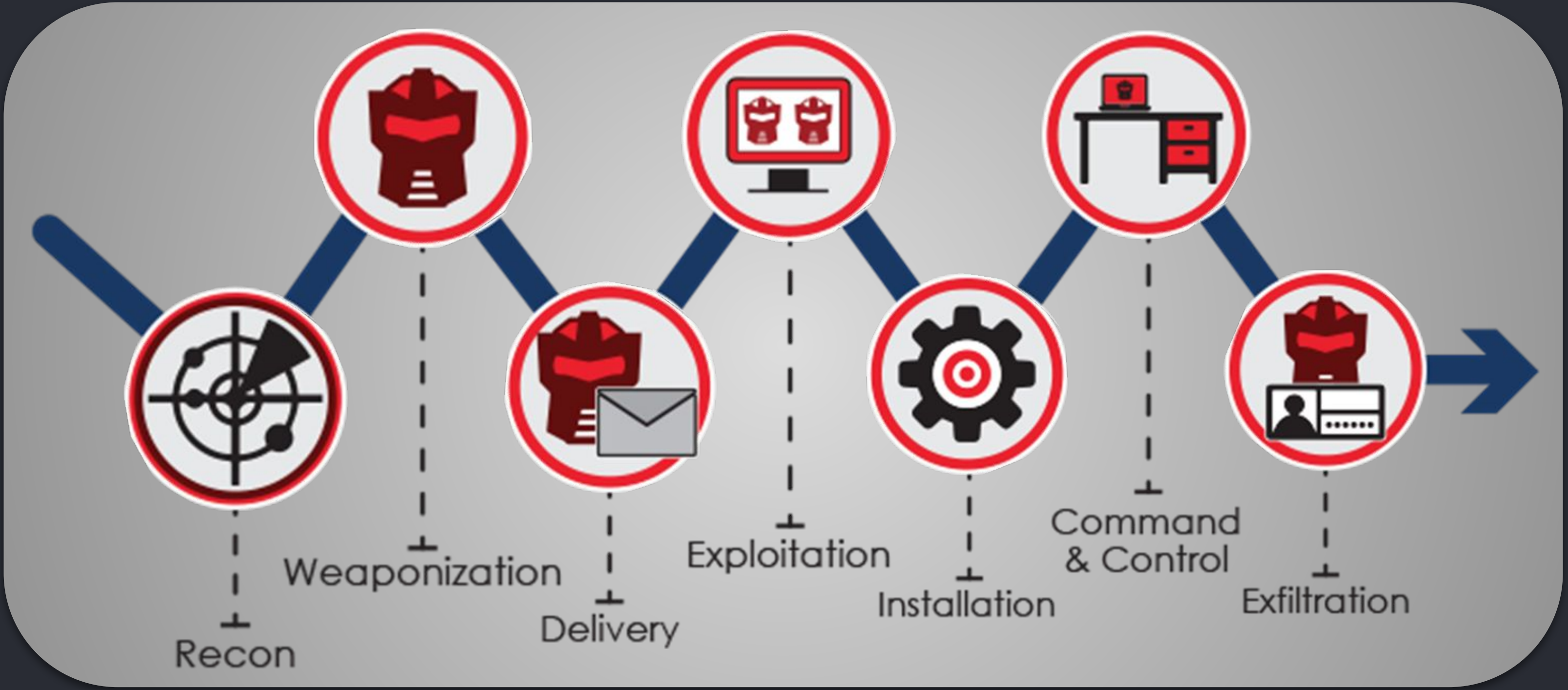
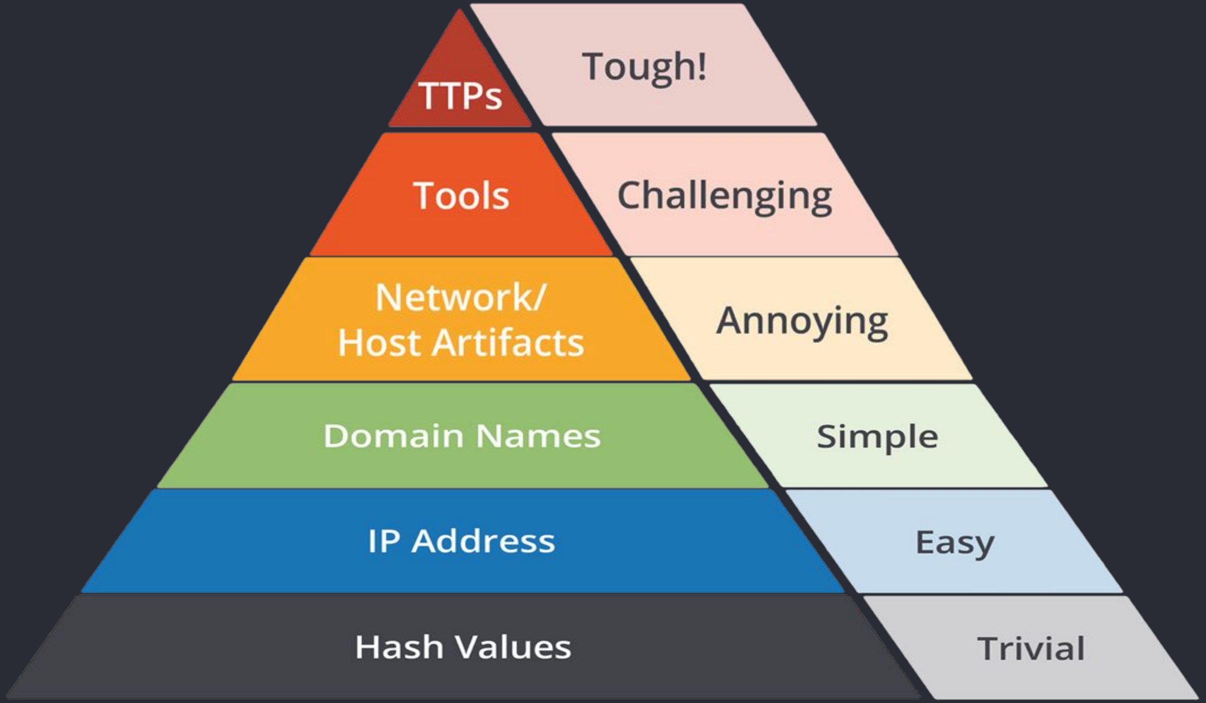
Operator Hunt

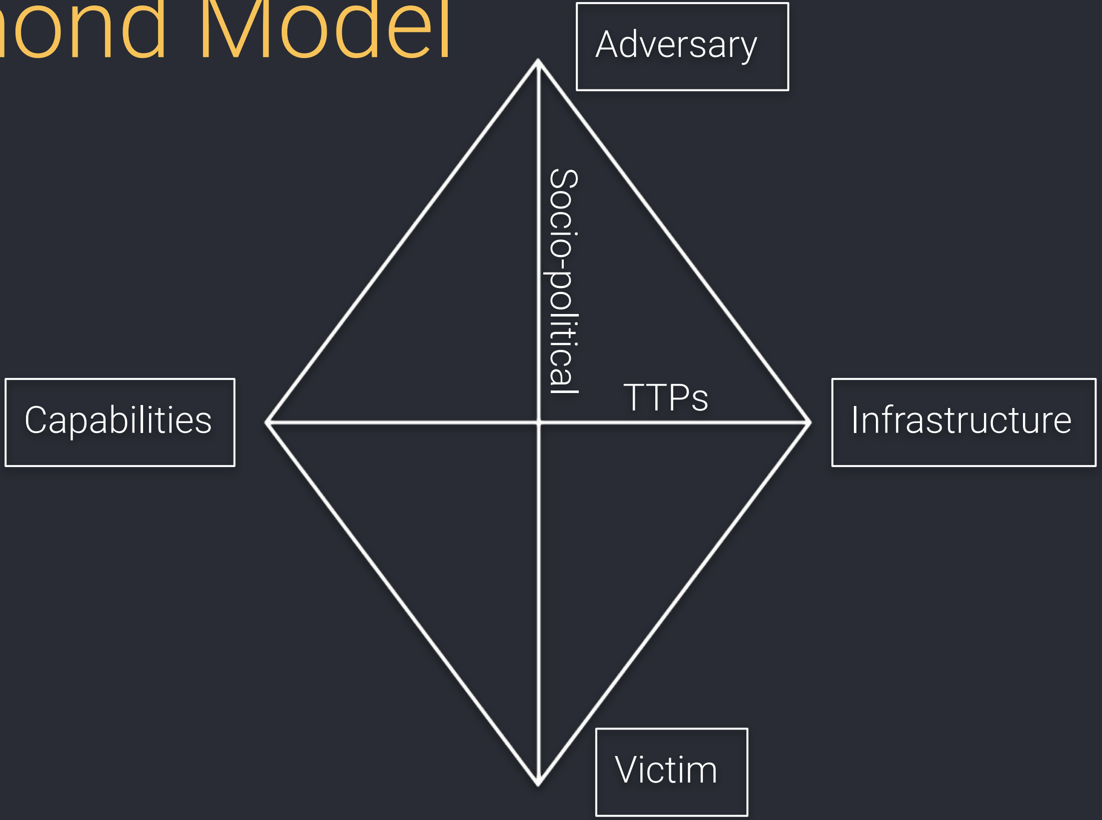
Cyber Kill Chain



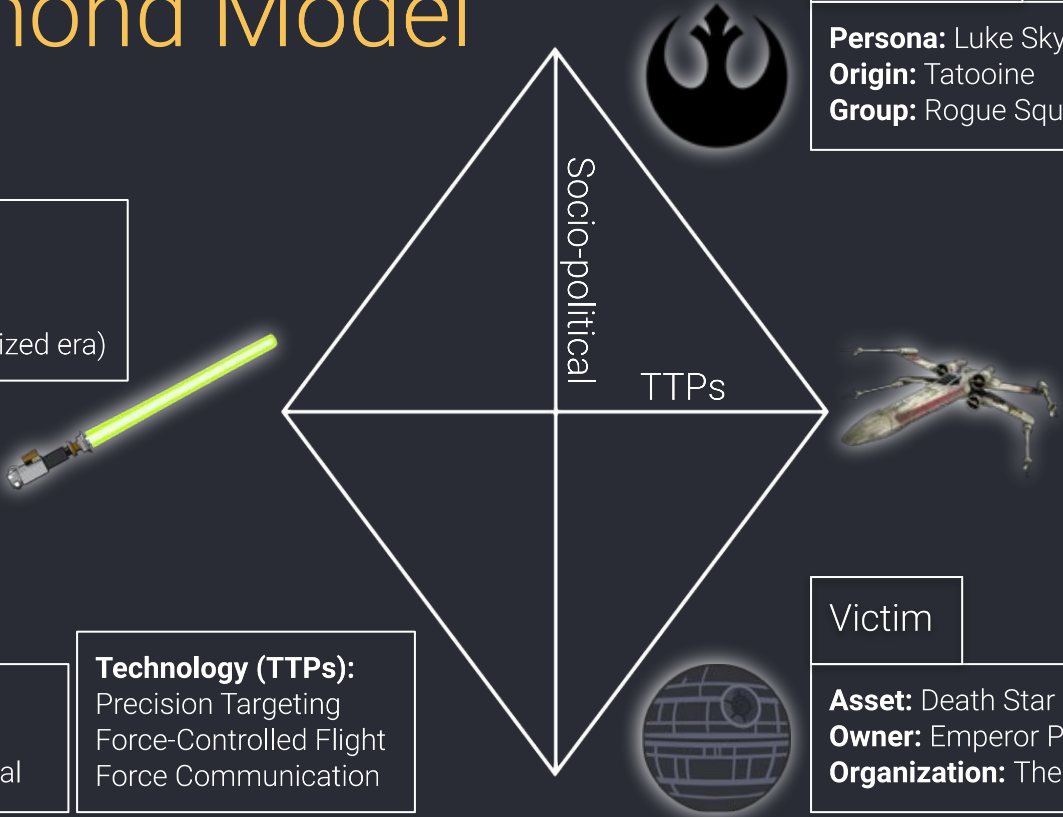
Pyramid of Pain



Diamond Model



Diamond Model



Adversary

Persona: Luke Skywalker
Origin: Tatooine
Group: Rogue Squadron, Rebel Alliance

Capabilities

The Force
Proton Torpedos
Anakin's Lightsaber
Blaster (from an uncivilized era)

Infrastructure

Yavin 4 (Rebel Base)
Fortressa (Carrier)
T-65 X-Wing (Fighter)
R2 D2 Astromech Droid

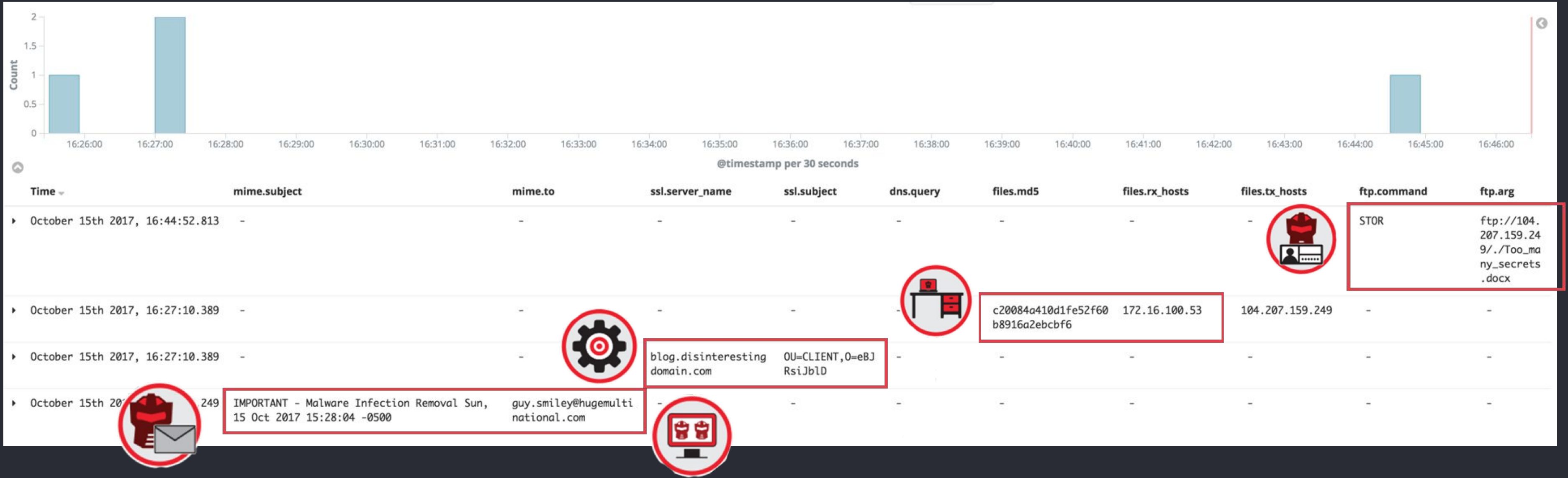
Victim

Asset: Death Star
Owner: Emperor Palpatine
Organization: The Empire

Socio-political:
Motive: Ideological
Intent: Political Upheaval

Technology (TTPs):
Precision Targeting
Force-Controlled Flight
Force Communication

Cyber Kill Chain - Example



Time	mime.subject	mime.to	ssl.server_name	ssl.subject	dns.query	files.md5	files.rx_hosts	files.tx_hosts	ftp.command	ftp.arg
October 15th 2017, 16:44:52.813	-	-	-	-	-	-	-	-	STOR	ftp://104.207.159.249/./Too_many_secrets.docx
October 15th 2017, 16:27:10.389	-	-	-	-	-	c20084a410d1fe52f60b8916a2ebcbf6	172.16.100.53	104.207.159.249	-	-
October 15th 2017, 16:27:10.389	-	-	blog.disinterestingdomain.com	OU=CLIENT,O=eBJRsiJblD	-	-	-	-	-	-
October 15th 20[illegible]249	IMPORTANT - Malware Infection Removal Sun, 15 Oct 2017 15:28:04 -0500	guy.smiley@hugemultinational.com	-	-	-	-	-	-	-	-

Operator | Hunt

	Reconnaissance	Weaponization	Delivery	Exploitation	Installation	Command & Control	Actions on Objective
OBSERVATIONS							
REMEDIATION							

CORP corporations network

- CORP is a small company lacking security professionals
- Their network is 172.16.100.0/24
- They have servers between 172.16.100.1-10
- They have client hosts between 172.16.100.50-254
- They have the following servers
  - Webserver - 172.16.100.4
  - Fileshare - 172.16.100.3
  - Domain Controller - 172.16.100.2

Resources Available

- RockNSM was deployed at CORP and the following data is available
  - Bro logs available via kibana
  - Suricata logs available via kibana
  - FSF logs available via kibana

- Kibana: http://classroom.perched.io:5601
- CTF: http://classroom.perched.io:8000

- Instructors able to answer questions regarding CORP assets or network

Attack #1

- Let's start out slow
- If you get stuck ask for help
- Instructors will give out hints periodically

- Time period of Activity
  - 2018-09-01 00:00:00.000
  - 2018-09-01 23:59:59.999

Attack #2

- Try to find this one on your own
- Ask instructor when you believe you have all the info
- Intel updates throughout the exercise

- Time period of Activity
  - 2018-09-02 00:00:00.000
  - 2018-09-02 23:59:59.999

Attack #3

- Try to find this one on your own
- Ask instructor when you believe you have all the info
- Intel updates throughout the exercise

- Time period of Activity
  - 2018-09-03 00:00:00.000
  - 2018-09-03 23:59:59.999

Attack #4

- Try to find this one on your own
- Instructor will act as team lead
- Instructor will update with live intel

- Time period of Activity
  - 2018-09-04 00:00:00.000
  - 2018-09-04 23:59:59.999

Attack #5

- This ones gonna be hard
- NO intel
- True hunting -- find what isn't normal
- Instructors will try to keep you out of the mud

- Time period of Activity
    - 2018-09-05 00:00:00.000
    - 2018-09-05 23:59:59.999