THREATCONNECT™

APPLYING THE DIAMOND MODEL FOR THREAT INTELLIGENCE TO THE STAR WARS' BATTLE OF YAVIN

Cyber Jedis know that Star Wars provides a wealth of incidents worthy of study. In fact, the entire story of *Episode IV: A New Hope* centers around the response to and consequences of a data breach, culminating in the destruction of the Death Star. If the Empire had been able to make sense of the intelligence they were gathering and had been able to connect the dots to reveal contextual information, they could have prevented their own demise, and stopped a decades-long saga from unfolding.

Watching the movie with your cyber-goggles on raises many interesting questions. Why didn't Vader recognize R2-D2 as the likely storage mechanism for the stolen plans? Why did the response team descend into bickering over ancient religions and eventual force-choking rather than dealing rationally and cooperatively with the situation? If they were such a critical external-facing vulnerability, why weren't the Death Star's exhaust ports better protected? Here, we've applied our intelligence methodology, the Diamond Model for Intrusion Analysis, to piece together the intelligence surrounding the Battle of Yavin and visualize what the Empire missed.

IF THE EMPEROR KNEW LUKE COULD TARGET WOMP RATS, MAYBE HE WOULD HAVE PROTECTED HIS EXHAUST PORT.

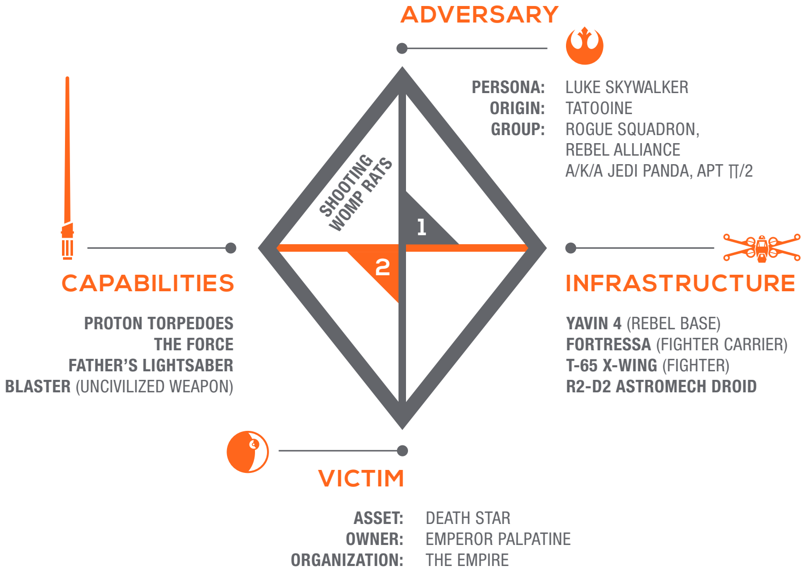
THE DIAMOND MODEL:

HOW IT WORKS

The DoD-derived Diamond Model is an approach to conducting intelligence on network intrusion events. The model gets its name (and shape) from the four core interconnected elements that comprise any event – adversary, infrastructure, capability, and victim. Thus, analyzing security incidents (or intrusions/activity threads/campaigns/ etc.) essentially involves piecing together "the Diamond" using bits of information collected about these four facets to understand the threat in its full and proper context.

THREATCONNECT INCIDENT 19770525F:

BATTLE OF YAVIN (EVENT: DEATH STAR DESTRUCTION)



ADVERSARY

PERSONA:	LUKE SKYWALKER
ORIGIN:	TATOOINE
GROUP:	ROGUE SQUADRON, REBEL ALLIANCE A/K/A JEDI PANDA, APT ∏/2

CAPABILITIES

PROTON TORPEDOES
THE FORCE
FATHER'S LIGHTSABER
BLASTER (UNCIVILIZED WEAPON)

INFRASTRUCTURE

YAVIN 4 (REBEL BASE)
FORTRESSA (FIGHTER CARRIER)
T-65 X-WING (FIGHTER)
R2-D2 ASTROMECH DROID

VICTIM

ASSET:	DEATH STAR
OWNER:	EMPEROR PALPATINE
ORGANIZATION:	THE EMPIRE

1 **SOCIO-POLITICAL AXIS**

MOTIVE: IDEOLOGICAL; REVENGE
INTENT: POLITICAL UPHEAVAL

2 **TECHNICAL AXIS (TTPS)**

PRECISION TARGETING
FORCE-CONTROLLED FLIGHT
FORCE COMMUNICATION

THREATCONNECT

INCIDENT 19770525F

It isn’t hard to imagine that if the Emperor had known Luke could bullseye womp rats in his T-16 back home on Tatooine, he might have surmised that he could also nail small exhaust ports from his much more capable X-Wing with the help of the Force. But apparently the Emperor didn’t know that, which constitutes a major intelligence failure, one that turned the tide of the war. The Empire would strike back, of course, but the inevitable return of the Jedi was set in motion. Had the Diamond Model been invented a long time ago in a galaxy far, far away, the outcome might have been different.

The Diamond Model diagram shows what the Empire could have reasonably known by assimilating the intelligence available to it at the time. The name of the incident underscores one of the pesky difficulties of incident analysis – dating. All we know of the Earth date of the incident is that it occurred “a long time ago.” We could go with the date of 0 BBY based on the Galactic Standard Calendar, but that has no relevance to Earthlings. Thus, we’ve adopted the day the incident became publicly known – May 25, 1977. “F” simply designates it as the 6th major incident of the day.

VICTIM

ASSET: DEATH STAR
OWNER: EMPEROR PALPATINE
ORGANIZATION: THE EMPIRE

We need not spend much time on the victim element of the Diamond. The Empire understood the power and value of its critical asset, the Death Star. Their reaction to the theft of the plans implies that they knew about the risk exposed by the exhaust port vulnerability, but apparently underestimated the adversary’s means of exploiting it.

ADVERSARY

PERSONA: LUKE SKYWALKER
ORIGIN: TATOOINE
GROUP: ROGUE SQUADRON,
REBEL ALLIANCE
A/K/A JEDI PANDA, APT ∏/2

From what can be gleaned from the movie, the Empire had decent intel on a key adversary persona, the young Skywalker. Enough, at least, to get a proper geolocation (thanks to his opsec failure of taking rooted machines home) and murder his known associates (of course, this should have tipped them off to the whole Anakin connection much earlier, but we won’t go down that rabbit hole right now). They also had pretty good knowledge of the Rebel Alliance, but were hampered by fuzzy attribution and their somewhat amorphous structure. Certain imperial units tried to genericize references to the Alliance by using “APT ∏/2,” while others emphasized the Force connection with the “Jedi Panda” moniker. We believe these naming inconsistencies led to confusion that effectively afforded the Alliance enough obscurity to continue offensive operations.

INFRASTRUCTURE

YAVIN 4 (REBEL BASE)
FORTRESSA (FIGHTER CARRIER)
T-65 X-WING (FIGHTER)
R2-D2 ASTROMECH DROID

We must assume the Empire had a high degree of knowledge about the Rebel infrastructure involved in the attack. They slyly allowed the Millennium Falcon to escape the Death Star and tracked it back to the Rebel base on Yavin 4. As they moved to execute the takedown operation, they undoubtedly knew of the Rebel’s carrier and fighter class ships, evidenced by the fact that they neutralized nearly all of them fairly quickly. It is likely, however, that the Empire did not realize that the Alliance had commandeered an astromech droid that had once belonged to one of its top military officials. The failure to contextualize this small piece of intelligence would later prove costly.

CAPABILITIES

PROTON TORPEDOES
THE FORCE
FATHER’S LIGHTSABER
BLASTER (UNCIVILIZED WEAPON)

That brings us to the final element in the Diamond Model, capability. The Empire knew the Alliance fighters could deploy proton torpedoes. Led by two Sith, they certainly knew about the Force. They knew about lightsabers and – even though they couldn’t hit anything with them – they knew about blasters too. No serious intelligence gaps here.

DOWNFALL OF THE DEATH STAR

While the Empire was missing key bits of information on some facets of the Diamond, their inability to make connections between the facets is what, quite literally, killed them in the end. The vertices between the points tie everything together and give the critical understanding of what the adversary wants and what they can do to accomplish it. In this light, it's clear that they failed to grasp the sum total of Luke's desire to revenge the death of his father (sssshhhh – remember he doesn't yet know), his natural precision targeting ability, his inherent strength in the Force, his covert channel communication with dead-but-still-alive ex-imperial generals, etc. Had they been able to put all this together, the story might have ended differently. Sure, we would probably have missed the awesomeness of *The Empire Strikes Back*, but we could have skipped all that screen time devoted to the Ewoks.

BUILD YOUR OWN ALLIANCE

After applying the Diamond Model to the Battle of Yavin, it is clear a Threat Intelligence Platform (TIP) like ThreatConnect could have helped the Empire avert catastrophe. In the case of the Empire, a TIP could have provided indicators and revealed context critical threats previously unseen. The same is true in your current business environment. ThreatConnect gives everyone in your organization – from the threat analysts, to incident response, to the CISO and CEO – a single platform to aggregate, analyze, and act on cyber threats. Where Darth Vader and the Emperor failed, you can succeed… in exploiting threat intelligence, that is. Nefarious interplanetary domination, is another story.

CONNECT WITH US

Interested in learning more about how ThreatConnect can help unite your security team and protect your enterprise?

SIGN UP FOR YOUR
FREE ACCOUNT

www.ThreatConnect.com/free

www.ThreatConnect.com

TOLL FREE: 1.800.965.2708
LOCAL: +1.703.229.4240
FAX: +1.703.229.4489

THREATCONNECT, INC.
3865 WILSON BLVD., SUITE 550
ARLINGTON, VA 22203

ABOUT THREATCONNECT

ThreatConnect is an enterprise solution that bridges incident response, defense, and threat analysis. Our premier cyber Threat Intelligence Platform allows global organizations to effectively manage the massive amounts of threat information that comes in daily. Organizations are able to move proactively against threats using ThreatConnect to increase productivity and deliver dynamic knowledge management, high context indicators, and automated responses. More than 5,000 users and organizations worldwide across industries, and ranging in size from the small business through the enterprise, turn to ThreatConnect to make intelligent decisions for their cyber security.