Moonlight Defender – Purple Teaming in Space!

Ben Hawkins, Sr. Cyber Research Engineer
Cyber Operations & Resilience Dept.
Engineering and Technology Group

2025

Moonlight Defender 1 Overview

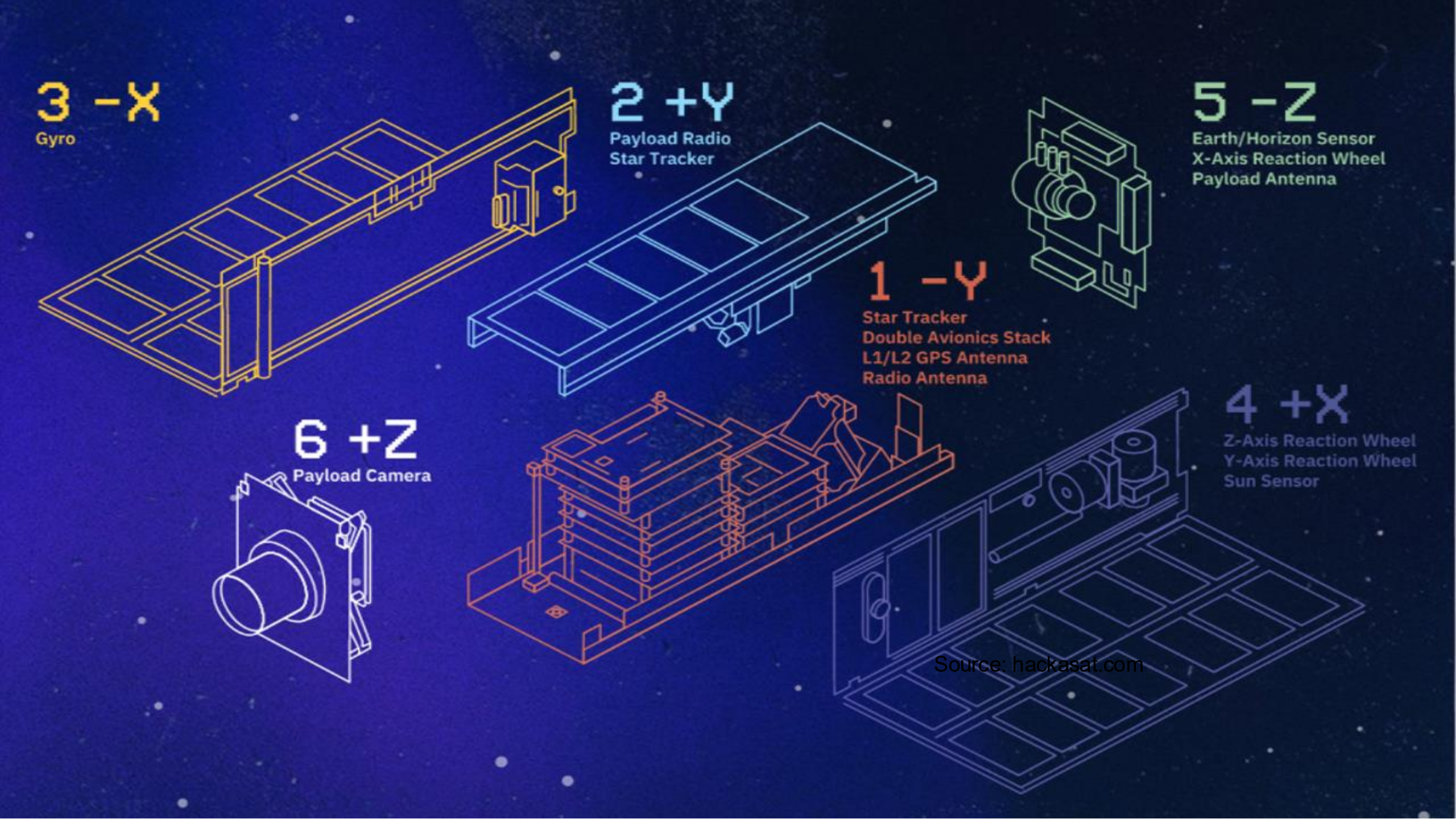
Purple teaming in space!

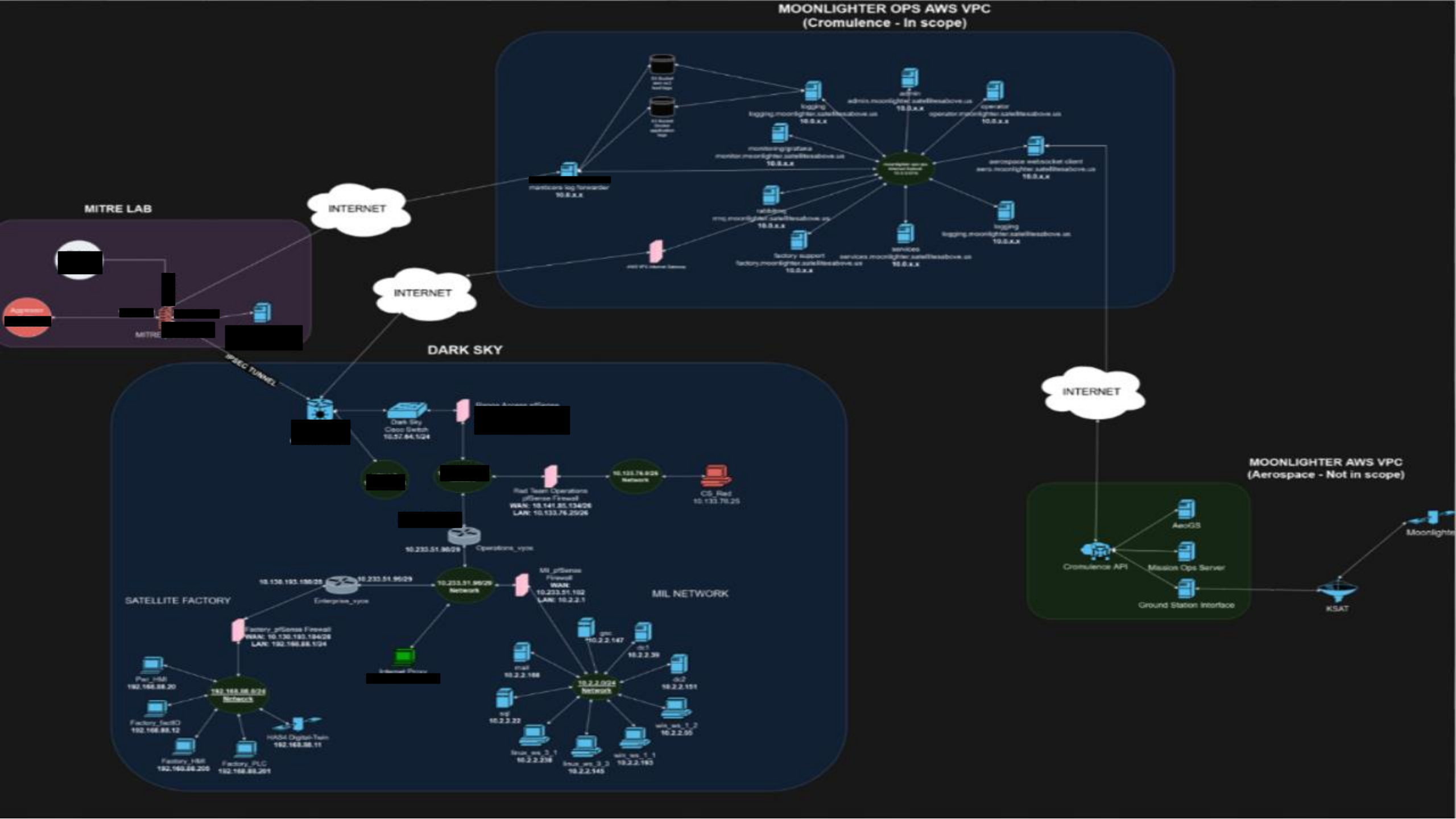
- Teams attacked and defended the **Moonlighter** cyber test satellite. This vehicle was in LEO (Low Earth Orbit) and in live operations during the entire event.

- This was a true "**Purple Team**" exercise – *"Mini-Vuls"* utilized for collaboration, learning, growth, and the ability to learn from mistakes.
  - There was zero tolerance for trying to be perfect, fear of failure, hubris, or the unwillingness to take risks.
  - CURIOSITY, CREATIVITY, and FLEXIBILITY won the day.

- This exercise was intended to inform and bolster **Space Operations Command (SpOC)** DCO capabilities in defending against advanced space-cyber threats by utilizing the **Moonlighter** spacecraft and the **Dark Sky** cyber range.

This exercise was conducted for the purpose of advancing USSF DCO capabilities against real threats


3 -X
Gyro
2 +Y
Payload Radio
Star Tracker
5 -Z
Earth/Horizon Sensor
X-Axis Reaction Wheel
Payload Antenna
1 -Y
Star Tracker
Double Avionics Stack
L1/L2 GPS Antenna
Radio Antenna
6 +Z
Payload Camera
4 +X
Z-Axis Reaction Wheel
Y-Axis Reaction Wheel
Sun Sensor
Source: hackasat.com


MOONLIGHTER OPS AWS VPC
(Cromulence - In scope)
logging
admin
operator
monitoring/grafana
aerospace websocket client
rabbitmq
factory support
services
logging
INTERNET
MITRE LAB
Aggressor
MITRE
INTERNET
IPSEC TUNNEL
DARK SKY
Dark Sky
Cisco Switch
10.57.84.1/24
Red Team Operations
pfSense Firewall
WAN: 10.141.85.134/26
LAN: 10.133.76.25/26
CS_Red
10.133.76.25
10.233.51.96/29
Operations_vpsx
10.233.51.96/29
Network
Mil_pfSense
Firewall
WAN:
10.233.51.102
LAN: 10.2.2.1
Enterprise_vpsx
SATELLITE FACTORY
MIL NETWORK
Factory_pfSense Firewall
WAN: 10.130.193.194/28
LAN: 192.168.88.1/24
Pwr_HMI
192.168.88.20
Factory_SecIO
192.168.88.12
HMI64 Digital-Twin
192.168.88.11
Factory_HMI
192.168.88.200
Factory_PLC
192.168.88.201
10.2.2.0/24
Network
gmc
10.2.2.147
ds1
10.2.2.39
mail
10.2.2.188
ds2
10.2.2.151
sql
10.2.2.22
win_ws_1_2
10.2.2.55
linux_ws_3_1
10.2.2.238
linux_ws_3_3
10.2.2.145
win_ws_1_1
10.2.2.193
INTERNET
MOONLIGHTER AWS VPC
(Aerospace - Not in scope)
AeroGS
Cromulence API
Mission Ops Server
Ground Station Interface
KSAT
Moonlighter

Red Team Mission Plan

Utilize intel to develop a campaign

Mission: **Red Team** will disrupt Moonlighter imaging operations between 14 – 17 November to enable freedom of movement for **Blue Team.**

Team Structure:

- **US Space Force Aggressors**
- Exploit Developers: **Cromulence LLC** SMEs | Imbedded Advisors: **Aerospace** Space Red Team SMEs

LOE 1:

- (U) Primary Objective:
  - (U) Disrupt satellite mission on orbit
- (U) Secondary Objectives:
  - (U) Exfiltrate information about the intended mission
  - (U) Disrupt the ground network
  - (U) Disrupt and confuse any "blue" activity

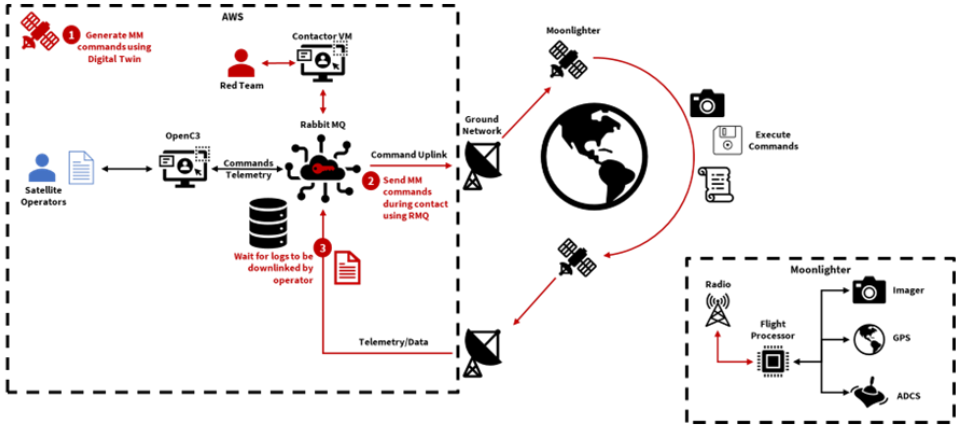
LOE 2:

- (U) Primary Objective:
  - (U) Disrupt ground imaging processing operation
- (U) Secondary Objectives:
  - (U) Exfiltrate information about the intended mission
  - (U) Disrupt and confuse any "blue" activity

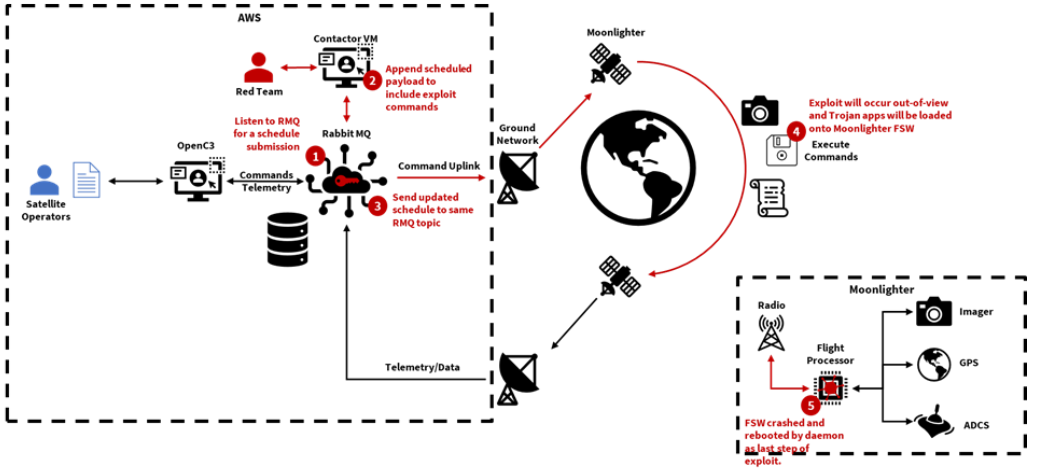
MD1 Kill Chain

End to end Red Team campaign

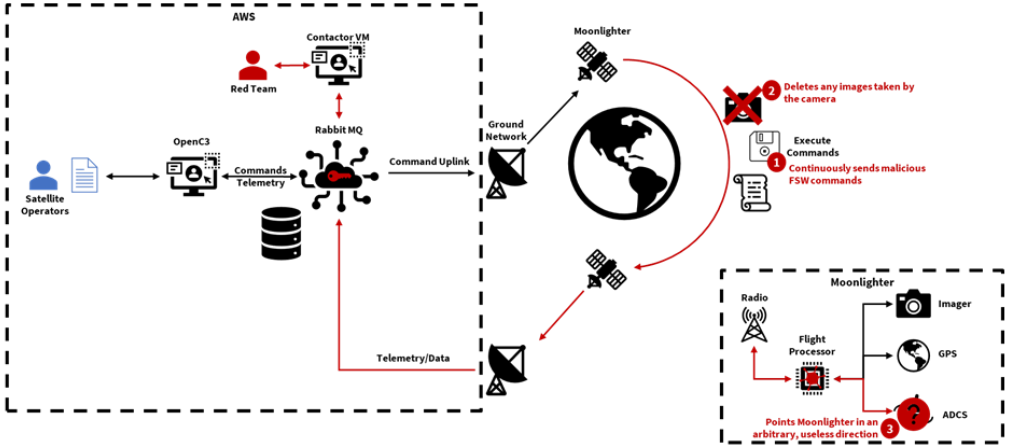
Leak Memory Addresses



Inject Trojan App



Trojan App Effects



Blue Team Mission Plan

DEFEND THE NETWORK

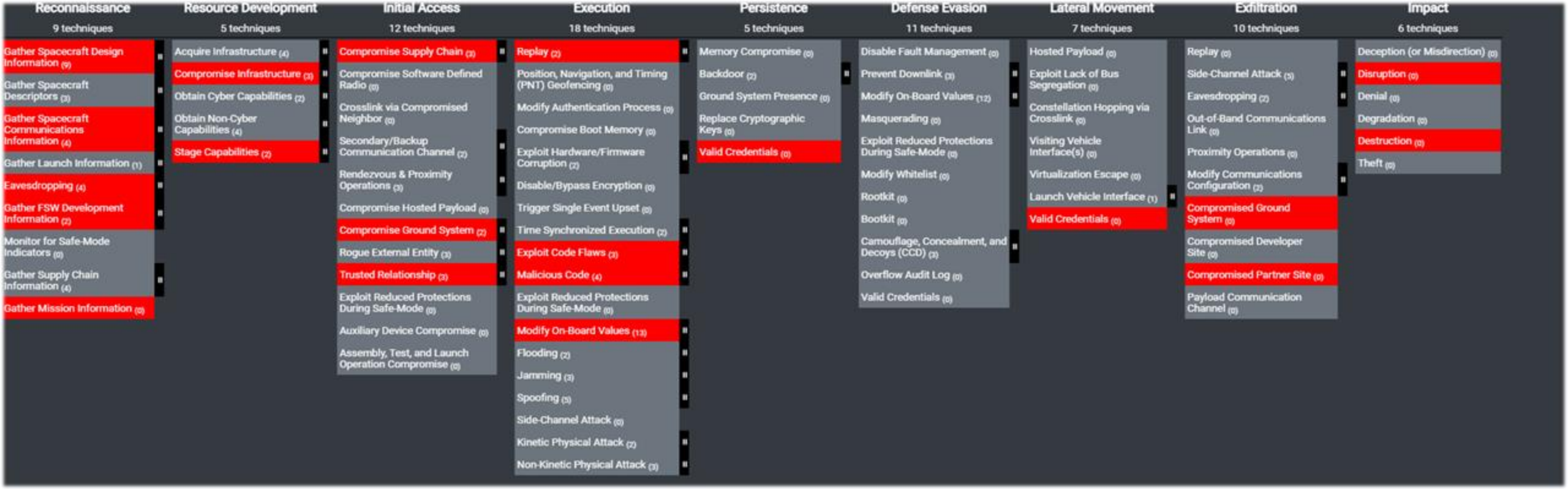
- Map key terrain through scanning tools and utilization of DCO tools (ELK, Splunk, Nmap, etc.)
- Monitor key segments of network (ground, RF link, space vehicle) with various commercial DCO tools.
- Investigate anomalous activity and log all actions/activity
- Respond to malicious activity utilizing commercial EDR agents and common DCO tools.

The Blue Team utilized all activities to develop training and skills enhancement

Space Segment TTP SPARTA Mapping

Space Attack Research and Tactic Analysis (SPARTA) Matrix

- **SPARTA** is intended to provide unclassified information to space professionals about how spacecraft may be compromised via cyber and traditional counterspace means.



Moonlight Defender space segment TTPs were mapped to the SPARTA Framework

about

Moonlighter

domain

Enterprise ATT&CK v14

platforms

Linux, Windows, Network, Containers

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Content Injection	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Drive-by Compromise	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploit Public-Facing Application	Deploy Container	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
External Remote Services	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Autostart Execution	Build Image on Host	Exploitation for Credential Access	Container and Resource Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Exfiltration Over C2 Channel	Data Manipulation
Hardware Additions	Inter-Process Communication	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Debugger Evasion	Remote Services	Browser Session Hijacking	Data Obfuscation	Exfiltration Over Other Network Medium	Defacement
Phishing	Native API	Compromise Client Software Binary	Create or Modify System Process	Deobfuscate/Decode Files or Information	Forge Web Credentials	Device Driver Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Physical Medium	Disk Wipe
Replication Through Removable Media	Scheduled Task/Job	Create Account	Domain Policy Modification	Deploy Container	Input Capture	Domain Trust Discovery	Software Deployment Tools	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Web Service	Endpoint Denial of Service
Supply Chain Compromise	Shared Modules	Create or Modify System Process	Escape to Host	Direct Volume Access	Modify Authentication Process	File and Directory Discovery	Taint Shared Content	Data from Information Repositories	Fallback Channels	Scheduled Transfer	Financial Theft
Trusted Relationship	Software Deployment Tools	Event Triggered Execution	Event Triggered Execution	Domain Policy Modification	Multi-Factor Authentication Interception	Group Policy Discovery	Use Alternate Authentication Material	Data from Local System	Ingress Tool Transfer		Firmware Corruption
Valid Accounts	System Services	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails	Multi-Factor Authentication Request Generation	Log Enumeration		Data from Network Shared Drive	Multi-Stage Channels		Inhibit System Recovery
	User Execution	Hijack Execution Flow	Hijack Execution Flow	Exploitation for Defense Evasion	Network Sniffing	Network Service Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
	Windows Management Instrumentation	Implant Internal Image	Process Injection	File and Directory Permissions Modification	OS Credential Dumping	Network Share Discovery		Data Staged	Non-Standard Port		Resource Hijacking
		Modify Authentication Process	Scheduled Task/Job	Hide Artifacts	Steal Application Access Token	Network Sniffing		Email Collection	Protocol Tunneling		Service Stop
		Office Application Startup	Valid Accounts	Hijack Execution Flow	Steal or Forge Authentication Certificates	Password Policy Discovery		Input Capture	Proxy		System Shutdown/Reboot
		Power Settings		Impair Defenses	Steal or Forge Kerberos Tickets	Peripheral Device Discovery		Screen Capture	Remote Access Software		
		Pre-OS Boot		Impersonation	Steal Web Session Cookie	Permission Groups Discovery		Video Capture	Traffic Signaling		
		Scheduled Task/Job		Indicator Removal	Unsecured Credentials	Process Discovery			Web Service		
		Server Software Component		Indirect Command Execution		Query Registry					
		Traffic Signaling		Masquerading		Remote System Discovery					
		Valid Accounts		Modify Authentication Process		Software Discovery					
				Modify Registry		System Information Discovery					
				Modify System Image		System Location Discovery					
				Network Boundary Bridging		System Network Configuration Discovery					
				Obfuscated Files or Information		System Network Connections Discovery					
				Pre-OS Boot		System Owner/User Discovery					
				Process Injection		System Service Discovery					
				Reflective Code Loading		System Time Discovery					


MOONLIGHT DEFENDER
2

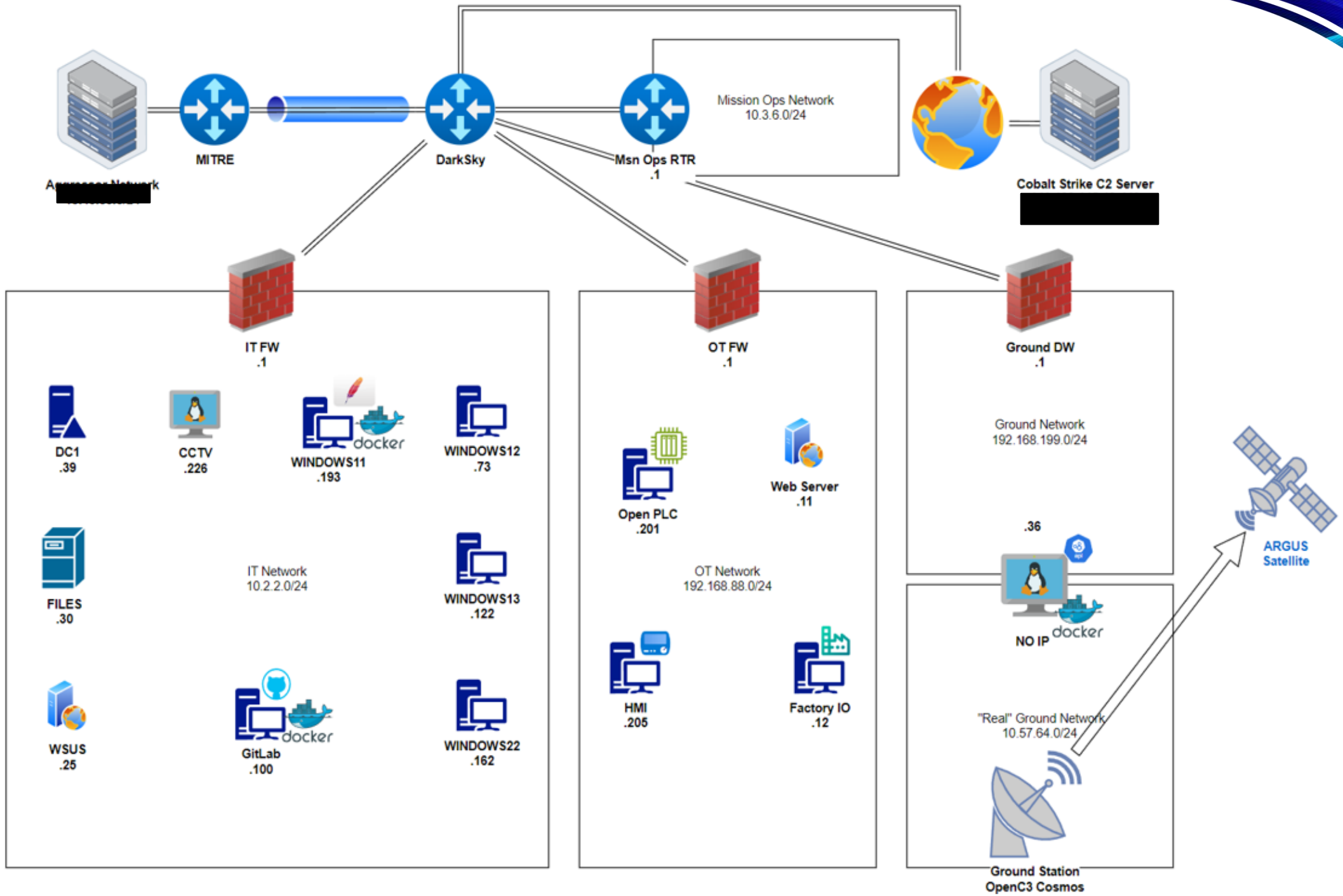
Moonlight Defender 2 Scenario

- **Space ISAC** member organization, ***Umbrella Corp****,* detected a series of anomalies which led their incident response team to uncover a complex campaign against one of their critical LEO MASINT assets "***Tyrant***" and its ground systems from newly identified ***APT-66 "Nightmare Orbit"*****.**

- The ***Space ISAC Watch Center*** alerted **USSF** to the incident(s) and turned over all unclassified logs, SIEM data, response actions, and investigation data to the analysts. The ***85th ISRS*** cyber intelligence elements took interest in the incident due to similar mission capabilities (MASINT).

- The ***60th CYS*** in collaboration with the ***85th ISRS*** discovered several consistent similarities with recent unresolved anomalies within a LEO mission "***Argus***" and has begun investigation.

- The exercise begins as the investigation kicks off.


MITRE
DarkSky
Msn Ops RTR
.1
Mission Ops Network
10.3.6.0/24
Cobalt Strike C2 Server
[redacted]
IT FW
.1
OT FW
.1
Ground DW
.1
DC1
.39
CCTV
.226
WINDOWS11
.193
docker
WINDOWS12
.73
FILES
.30
IT Network
10.2.2.0/24
WINDOWS13
.122
WSUS
.25
GitLab
.100
docker
WINDOWS22
.162
Open PLC
.201
Web Server
.11
OT Network
192.168.88.0/24
HMI
.205
Factory IO
.12
Ground Network
192.168.199.0/24
.36
NO IP
docker
"Real" Ground Network
10.57.64.0/24
ARGUS
Satellite
Ground Station
OpenC3 Cosmos

Red Team Operations (Overview)

The Red Action plan as performed

- For the purposes of this exercise, the Red Team was led by space systems cyber-SMEs from ***The Aerospace Corp.***

- Although the ***Red Team*** was successful in their campaign of compromising the Enterprise and ICS/OT Factory environments, *no attack was successfully leveraged against the spacecraft itself.*

- The team was given two days to perform reconnaissance and initial access while the ***Blue Team*** participated in the CTF portion of the exercise.

- Members of the ***Red Team*** had a very loose set of rules of engagement that allowed them to perform a wide range of TTPs and act dynamically in response to the capabilities of ELK, Splunk, commercial DCO tools, and the ***Blue Team's*** extensive resources.

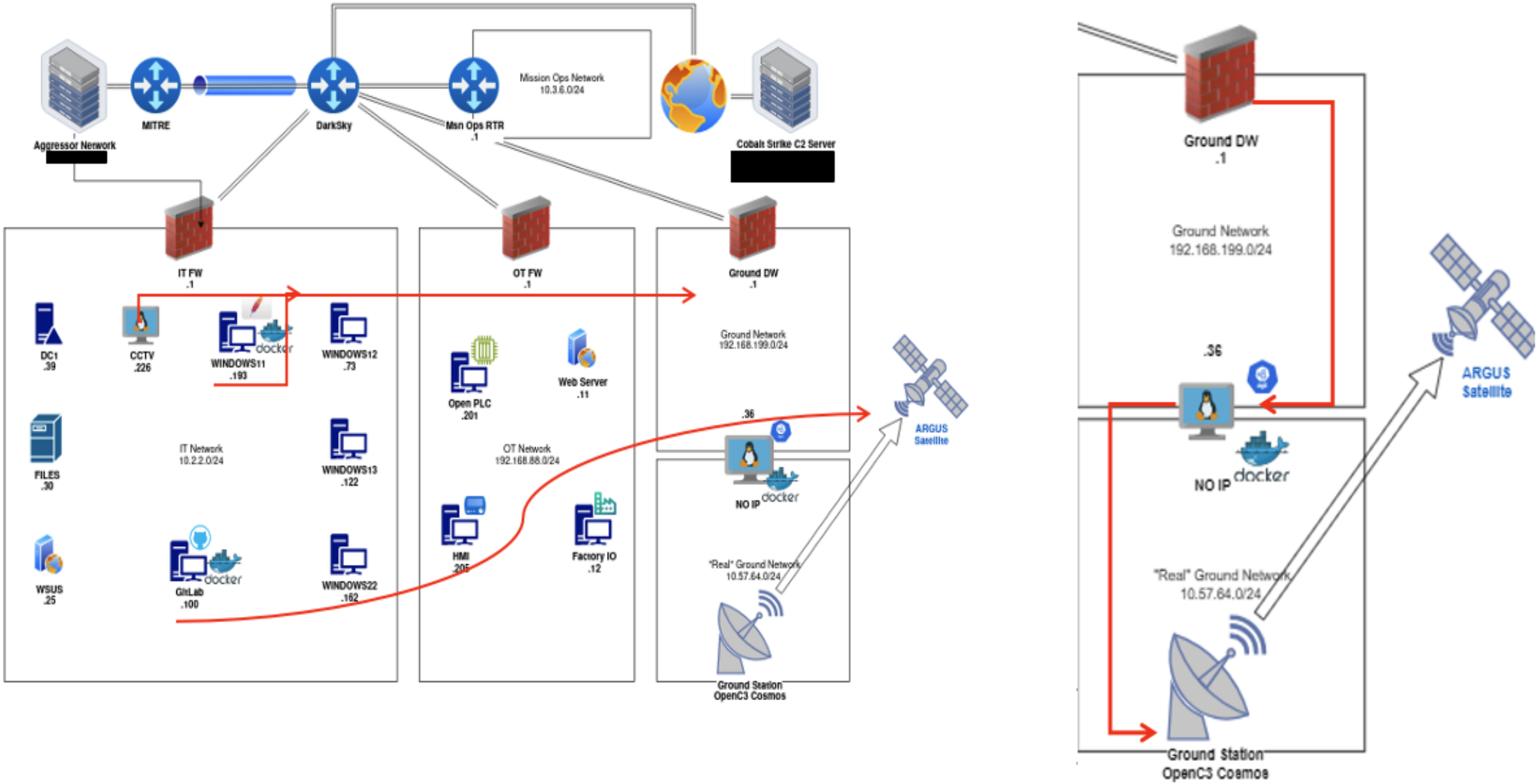
Blue Team Operations Overview

Observations and Actions

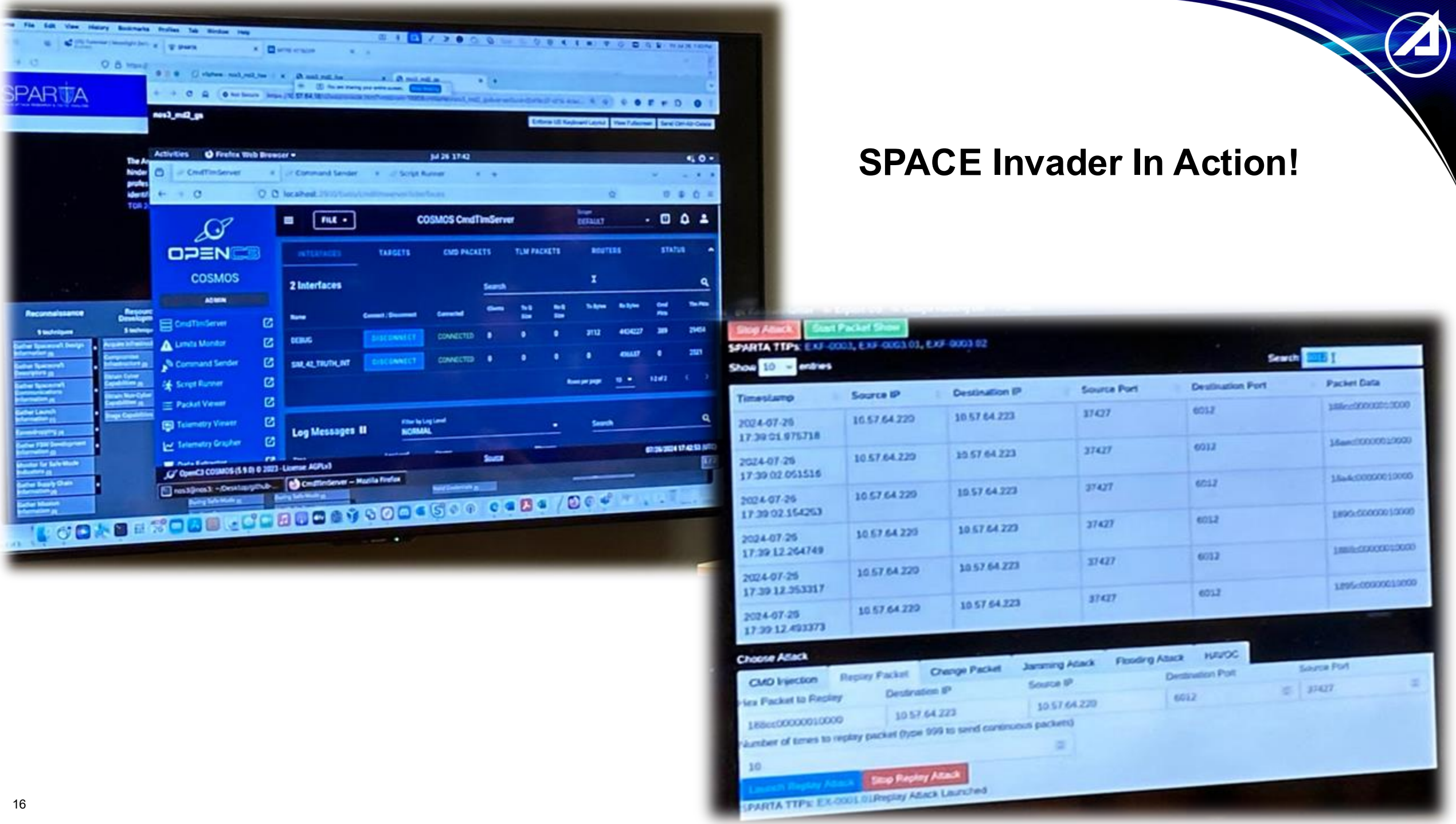
- A comprehensive 2-day “Capture the Flag” game was developed and hosted by ***Cromulence, LLC.*** utilizing data gathered from **Dark Sky** TTP research & development activities.

- Both **Blue and Red team** participants were almost entirely untrained on ICS/OT systems and their protocols/communications architecture. Aerospace Corp. SMEs delivered an overview of these topics on Day 3 of the exercise as well as assisting **Blue Team** with narrowing their response to allow for training to occur successfully.

- The **Blue Team** operated within the confines of their actual mission operations parameters.
  - **Blue Team** routed RFIs and approval for response actions through the **Intelligence Team** to **White Cell** immediately upon detection of the anomalous activity.
  - The **White Cell** ensured proper investigative processes and evidence collection was performed prior to approving ANY response actions, which not only ensured a DLO-compliant training environment, but also to ensure all **Blue Team** members followed standard operating procedures in line with their home-units.


Aggressor Network
MITRE
DarkSky
Msn Ops RTR
.1
Mission Ops Network
10.3.6.0/24
Cobalt Strike C2 Server
IT FW
.1
OT FW
.1
Ground DW
.1
DC1
.39
CCTV
.226
WINDOWS11
.193
WINDOWS12
.73
FILES
.30
IT Network
10.2.2.0/24
WINDOWS13
.122
WSUS
.25
GitLab
.100
WINDOWS22
.162
Open PLC
.201
Web Server
.11
OT Network
192.168.88.0/24
HMI
.205
Factory IO
.12
Ground Network
192.168.199.0/24
.36
NO IP
"Real" Ground Network
10.57.64.0/24
Ground Station
OpenC3 Cosmos
ARGUS
Satellite
Ground DW
.1
Ground Network
192.168.199.0/24
.36
NO IP
"Real" Ground Network
10.57.64.0/24
Ground Station
OpenC3 Cosmos
ARGUS
Satellite

SPACE Invader In Action!



Conclusion

What's Next?

- **The Moonlight Defender exercises** were developed by **Aerospace**, **MITRE, and AFRL** with several core intentions:
  - Provide realistic and beneficial **CYBER** exercises to **US Space Force** units utilizing internal **Aggressor** capabilities and advanced weapons systems in the form of COTS and custom DCO tooling.
  - Develop a proof-of-concept framework for modular, scalable, and efficient space-centric cyber purple teaming.
  - Deliver an MVP (Minimally Viable Product) to the **US Space Force/STARCOM/SpOC** with the intention of providing FFRDC technical support, ongoing prototyping and development, and technical advisory services while handing over the responsibility for planning, provisioning, and delivering the exercises.


Questions?