ICS Sec for n00bz:
An Introduction to ICS Security by Defending the Death Star

Kara Turner
First Order IT Training

- Welcome!
- Starkiller Base
Purpose of Training

- Lessons Learned from Death Star
- Don’t let this one blow up.
ICS Aboard the Death Star
ICS on the Death Star

- Sensors and Actuators:
  - Doors
  - Tie Fighter Conveyor

INDIGNITY

We all can’t walk through the passageway of life without hitting our heads on the door of humiliation.
ICS on the Death Star

- PLC:
  - Weapons Factory Automation
  - Lighting Fixtures
  - Bacta Tanks
  - Turbo lifts
ICS on the Death Star

- Humanoid Machine Interface
  - No GUI
  - Interfaced with controllers operating processes
    - Turbo Lift
    - Darth Vader’s breathing apparatus
ICS on the Death Star

- Control Room:
Blocking Access
Block Rebel Scum Access to Death Star Networks

- If it is crucial to the mission or improves efficiency without compromising security, allow access - block everything else
- Just because most people don’t know how it works doesn’t mean a slicer can’t figure it out
ICS Defense: Blocking Access

Disable unnecessary open ports

- No more Wookiefy on ICS servers
Application Whitelisting

- Ensure that only authorized communications occur between programs
  - Food production programs should not communicate with the weapons controls
  - Weapons controls should communicate with emergency systems
ICS Defense: Blocking Access

- Block Rebel Scum Access to Death Star Networks
  - Disable unnecessary open ports
  - No more Wookiefy to listen to cantina bands on ICS network
- Application Whitelisting
  - Food production system should not be communicating with the weapons controls
Authentication Policy

- No shared credentials
  - Traceability
  - Accountability
- No Default Passwords
- 2 Factor Authentication
  - ID chip in each helmet and passcode
ICS Defense: Blocking Access

Within the Network:

- Use firewalls to segment the network
  - Corporate Empire Network
  - DMZ
  - ICS network
Monitoring
When in doubt, Log it

Access Logs

- Unusual User Behavior
  - Account used while on PTO or at unusual hours?
  - Account used while owner dead
ICS Defense: Monitoring

Network Baseline

- Behavioral Analysis
  - Determine expected behaviors
  - Generate alerts when standard deviation is exceeded
  - Services communicating on ports they don’t usually use
ICS Defense: Risk Management

Identify Weaknesses

- Death Star was not invincible, neither is Starkiller Base
  - Death Star plans captured
  - Assumed the enemy is unable to read them
  - Rebels found weakness and exploited it
  - Should have anticipated Rebel objectives
Identify Weaknesses

- Hardcoded/Weak/Old Passwords
- System Patches
  - Monitor Feeds
  - Determine risk/cost of applying patch versus abstaining
Social Engineering Awareness

- Rebel agents steal Empire uniforms, pass undetected
Threat Intelligence

- Know your enemy
- Monitor their movements
- Monitor the environment
Risk Assessments

- No single point of failure
- Determine safeguards
- Empire built second Death Star
- Hot Site/Cold Site
Incident Response Planning

- Knew the Rebels had Death Star plans
- Response not adequate to counter threat
Multiple Solutions

- Something will fail
- Different perspectives provide greater coverage
All images were captured from Star Wars, episodes 4-7, derivatives thereof, or fan creations concerning the Star Wars franchise: