THREAT MODELING STAR WARS EDITION

Audrey Long

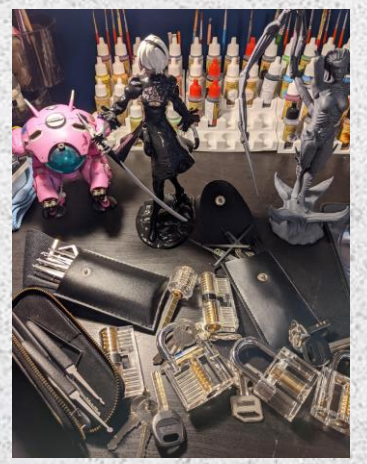
Sr. Security Software Engineer

My Favorite Book Series

I Love Cooking, Creating, and Learning

Women Techmakers

Google



University of CINCINNATI

JOHNS HOPKINS UNIVERSITY

My Favorite Games

OVERVIEW

- By the end of this session, we will:
- Obtain a Security Mindset
- Gain Threat Modeling Fundamentals
- Walk Through the Steps to Generate Threat Models
- Threat Model the Death Star
- Obtain Cool Security Knowledge!

WHAT IS THREAT MODELING?

- Threat Modeling takes an adversarial view of a system, exposes potential security threats in the design, and presents measures to mitigate them
- Threat modeling is, in essence, the act of creating a security design specification for an application

WHO SHOULD BE THREAT MODELING?

Software Engineers

Security Engineers

Architects

Program Managers

Software Testers

Anyone with a Working Knowledge of the System

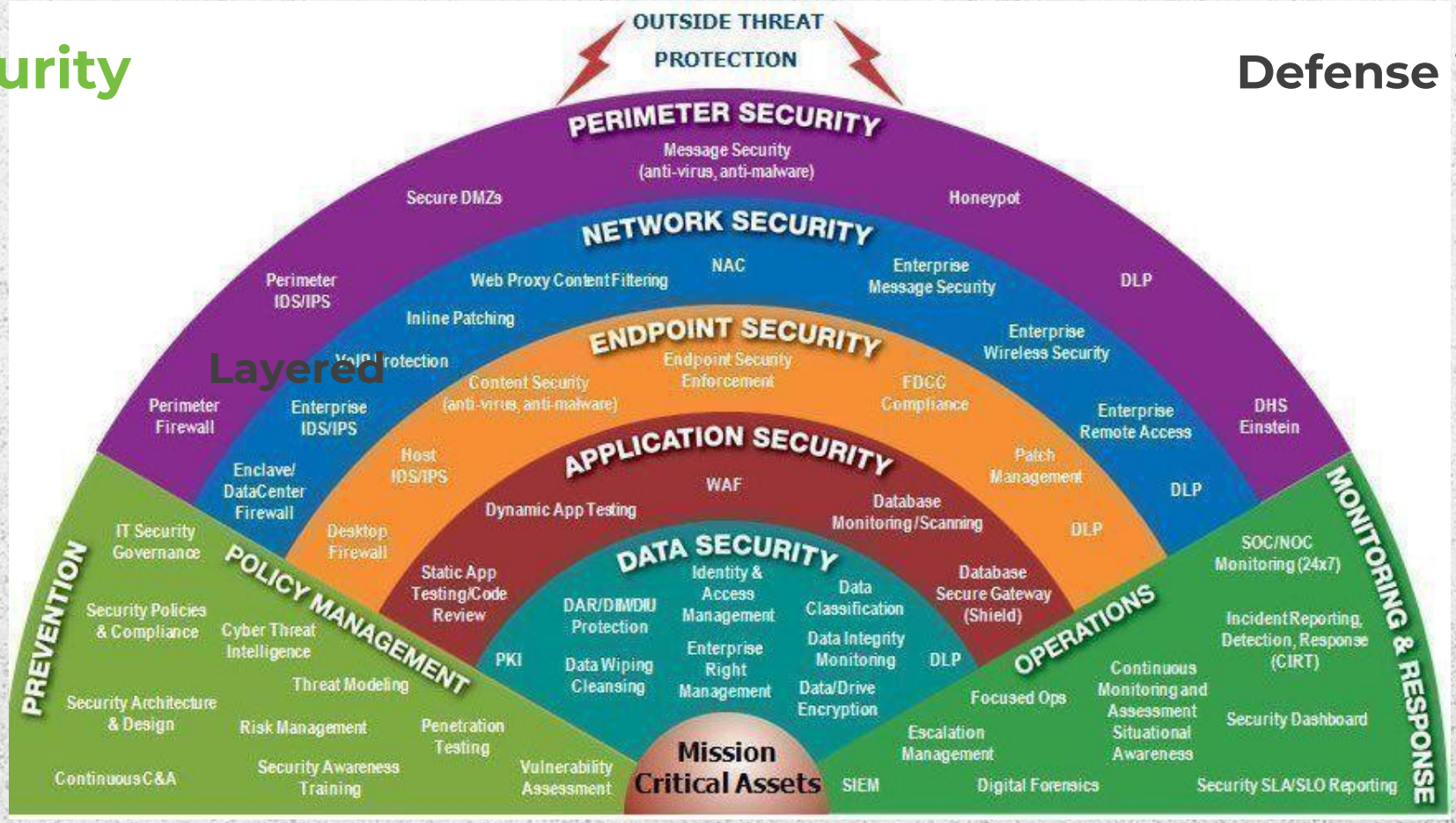
WHEN SHOULD WE CREATE THREAT MODELS?

- Best applied during design
- Creating a new cloud application or microservice
- Designing a public API to provide customers access to your data
- Adding a new feature to an existing application
- Creating a new cloud infrastructure project

SECURITY FOUNDATIONS

Layered **Security**

Defense in Depth



MICROSOFT SECURITY DEVELOPMENT LIFECYCLE

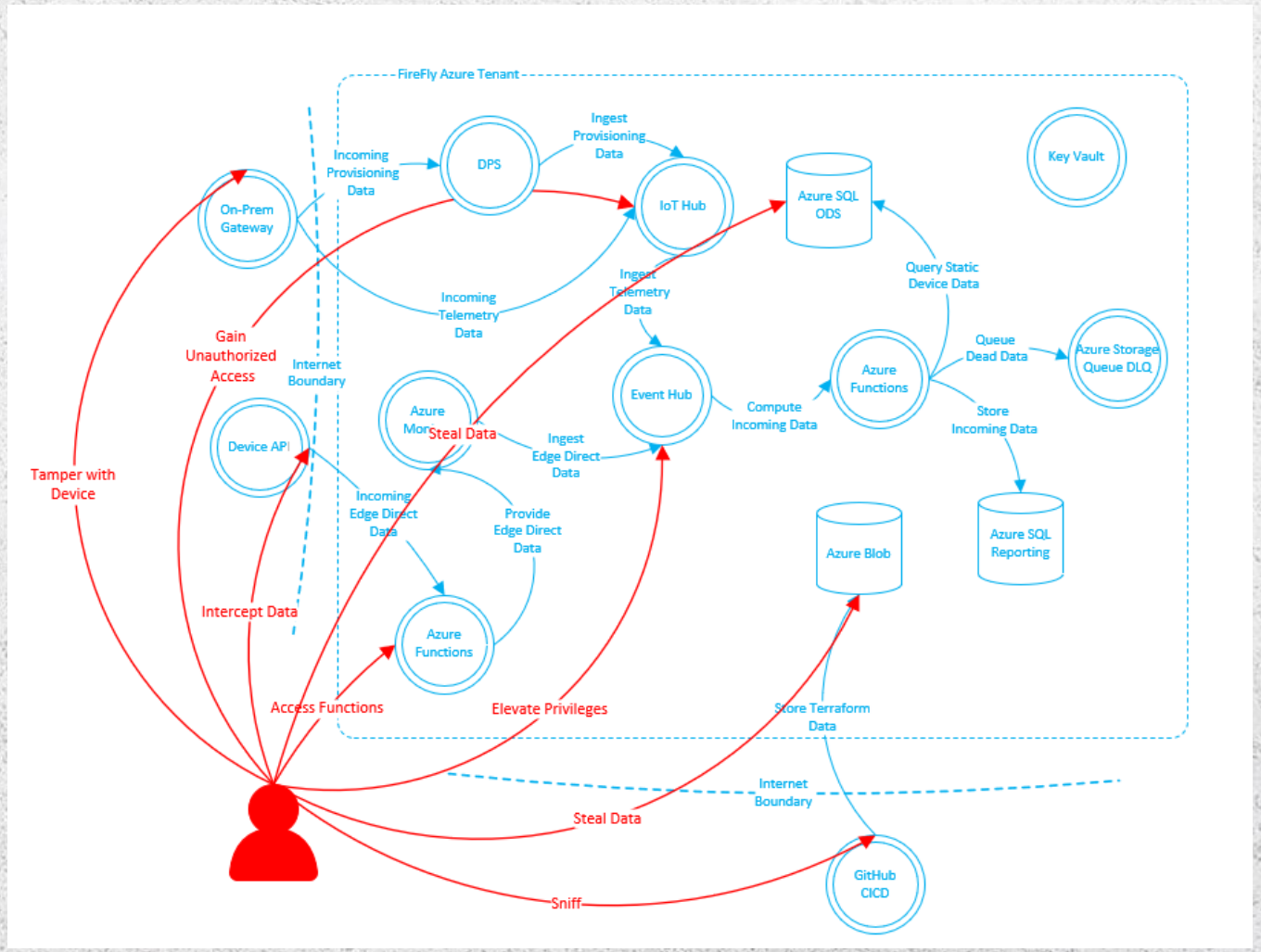
Provide	Define	Define	Perform	Establish	Define	Manage	Use	Perform	Establish
Provide Security Training	**Define Security Requirements**	**Define Metrics and Reporting**	**Perform Threat Modeling**	**Establish Design Requirements**	**Define and Use Crypto Standards**	**Manage the Security Risk of using Third Party Components**	**Use Approved Tools**	**Perform Static Analysis, Dynamic Analysis, and Pen Testing**	**Establish a Standard Incident Response Process**
									

SECURITY MINDSET

Good engineering involves thinking about how things can be made to work

The security mindset involves thinking about how things can be made to fail

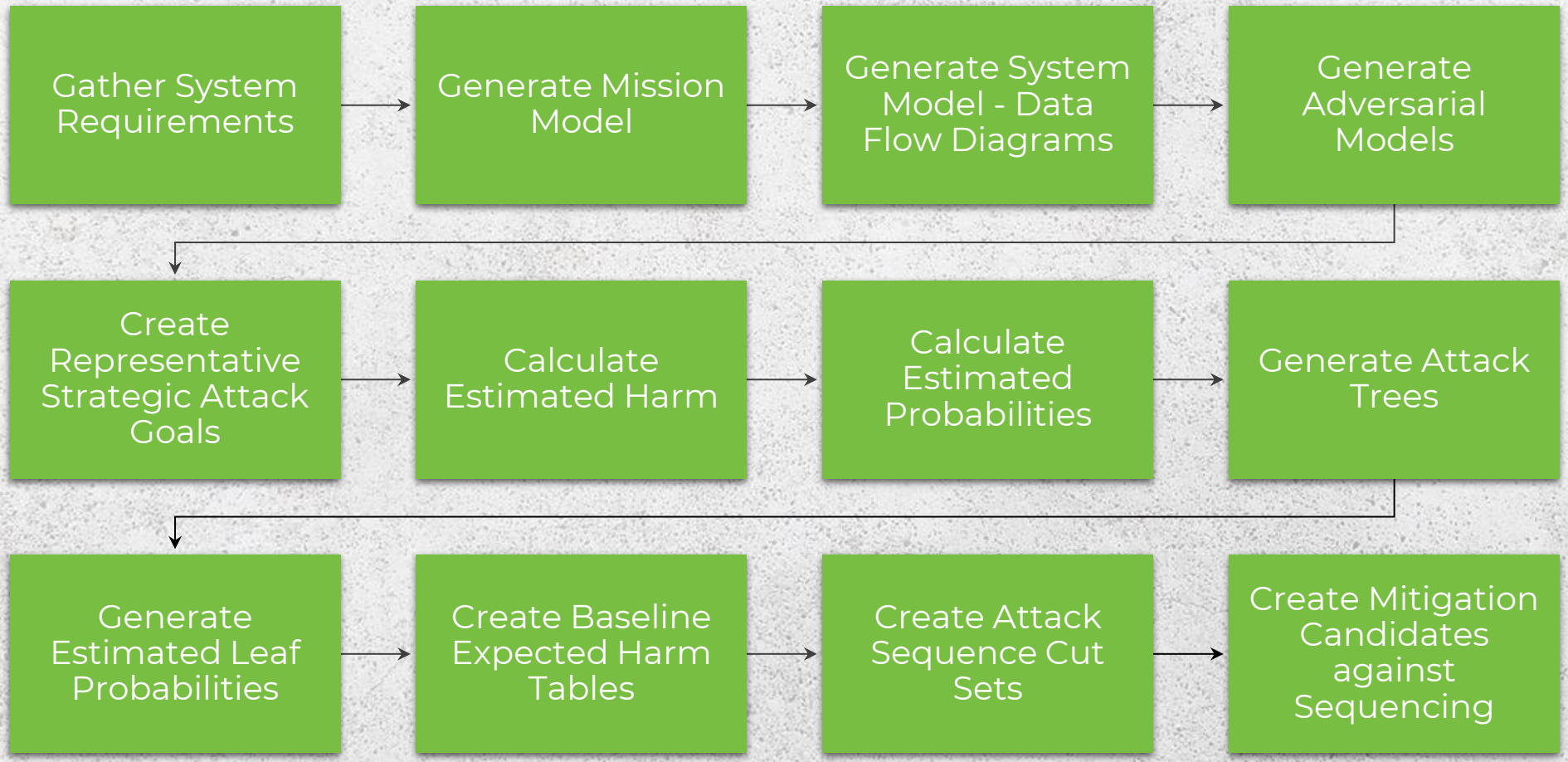
[The Security Mindset - Schneier on Security]



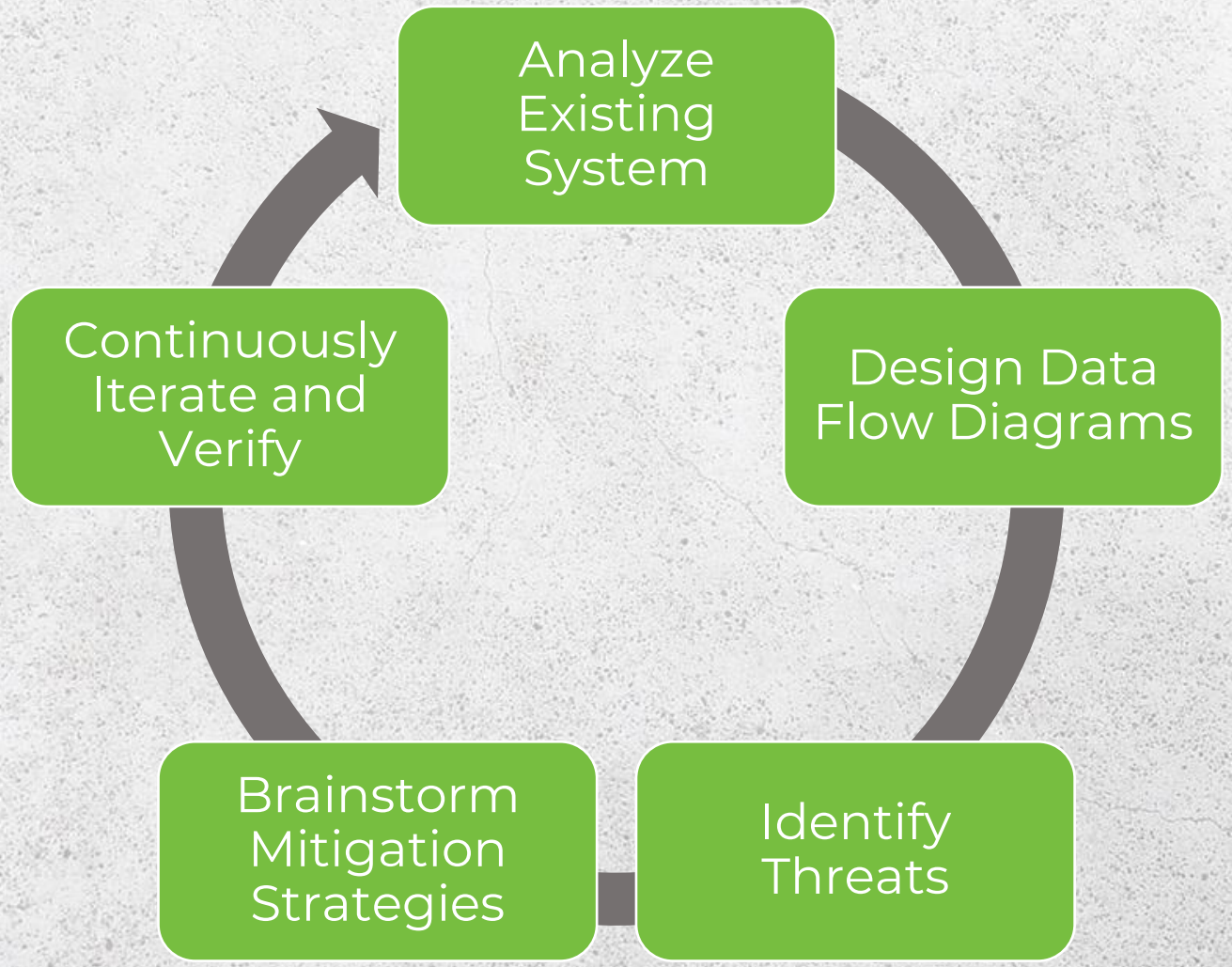
ADVERSARIAL THREAT MODELING

#	Adversary Class	Key Characteristics
1	Nation-state at peace	Long-term, espionage and influence focused, well-resourced, risk-averse
2	Nation-state at war	Short-term, sabotage and influence focused with targeted espionage, well-resourced, risk-tolerant
3	Transnational terrorists	Short-term, sabotage-focused, well-resourced, risk-tolerant
4	Organized crime	Well-resourced, risk-averse, financial-focused
5	Hacktivist	Very high skills, activist-oriented, modest resources
6	State-tolerated hacker groups	Very high skills, nation-state type goals, modest resources, though sometimes subsidized by nation-states
7	Lone hacker	Innovative, determined, risk-averse

CLASSICAL THREAT MODELING – 1000FT PERSPECTIVE



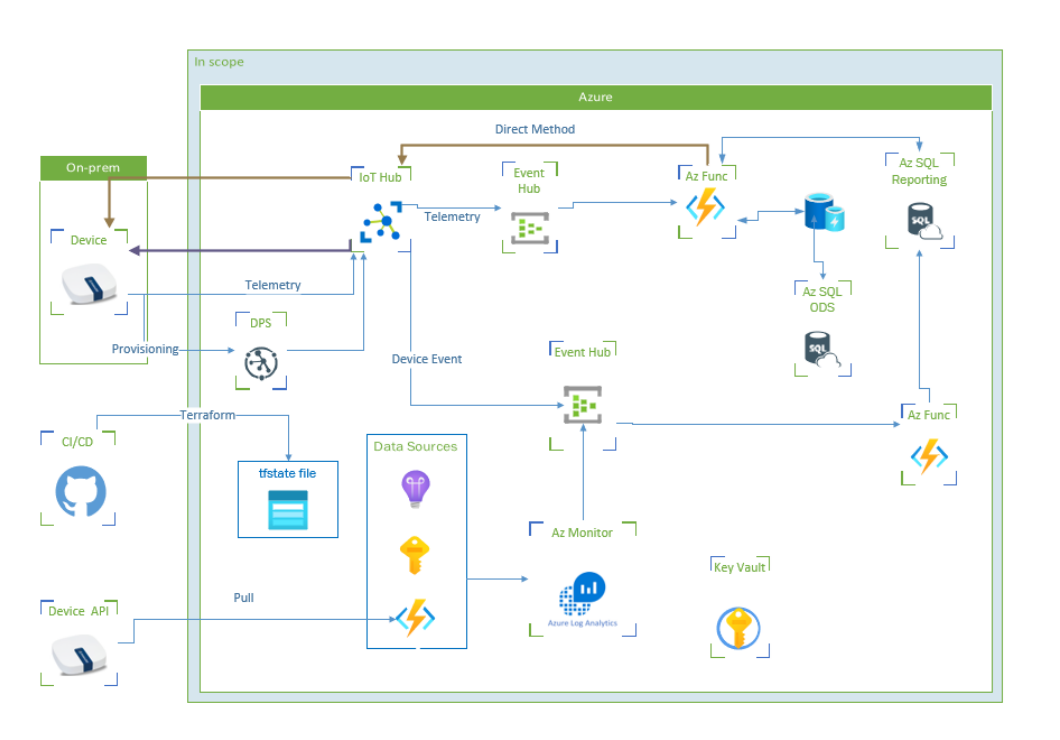
PHASES OF THREAT MODELING



1 – ANALYZE THE SYSTEM

Goals

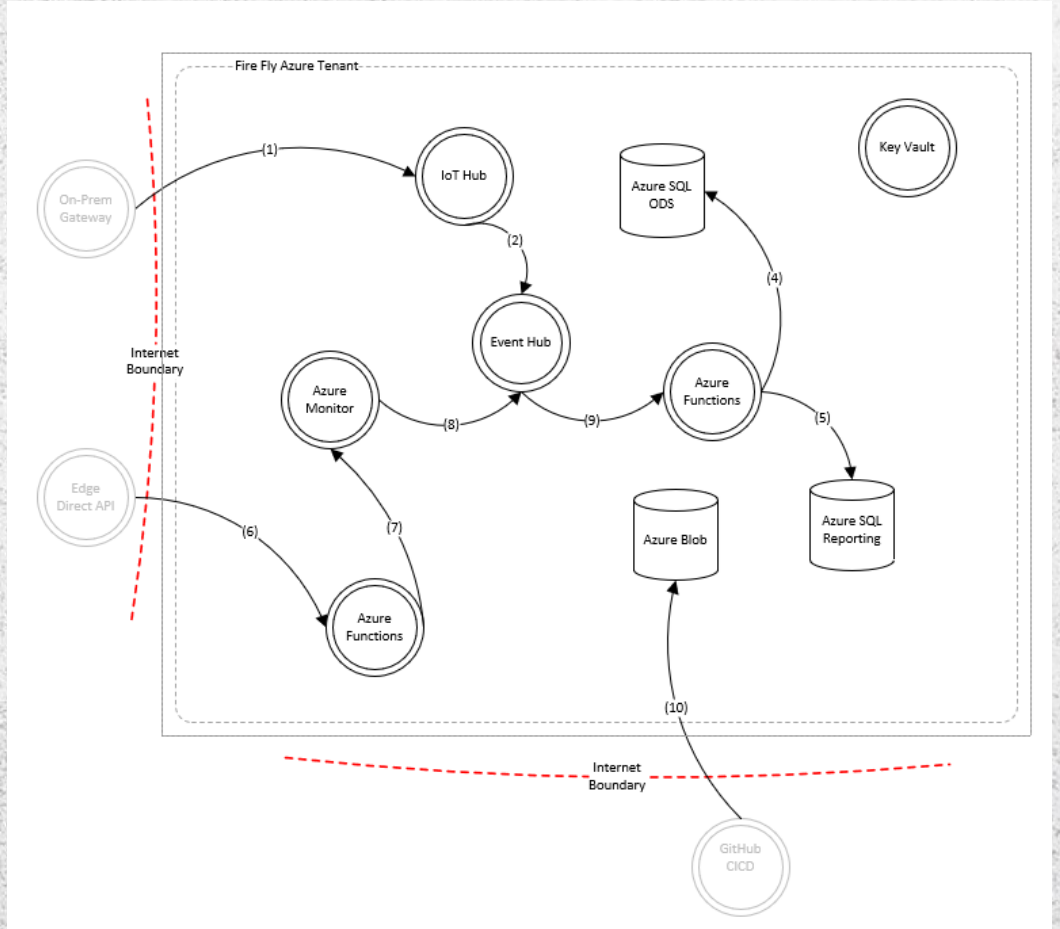
- Develop a clear picture of how your system nominally functions
- Enumerate services consumed by your system
- Investigate environment assumptions and security controls
- Gather system requirements documents
- Identify key security stakeholders



2 – DESIGN A DATAFLOW DIAGRAM

Goals

- Understand the user and system scenarios throughout the system
- Establish trust zones and boundaries within your system
- Identify user permissions used throughout the system lifecycle
- Investigate protocols being used inside and outside of the system being designed



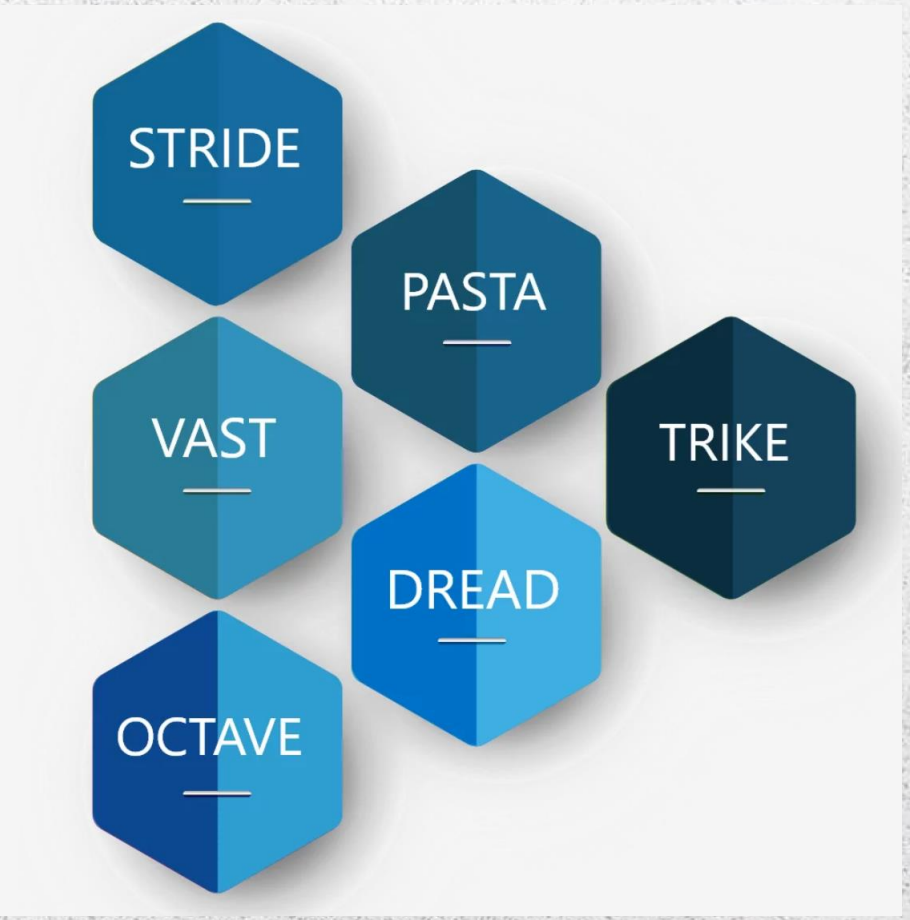
STANDARD DFD ELEMENTS

Element	Shape	Definition	Example
Process		Task that receives, modifies, or redirects input to output	Web service
Data store		Permanent and temporary data storage	Web cache and Azure DB
External entity		Task, entity, or data store outside of your direct control	Users and third-party APIs
Data-flow		Data movement between processes, data stores, and external entities	Connection strings and payloads
Trust boundary		Trust zone changes as data flows through the system	Users connecting to a secured corporate network over the internet

3 – IDENTIFY THREATS

Goals

- Apply your security mindset
- Choose whether you want to find ways to protect your system, or you want to understand all you can about an attacker and their motives
- Use the data flow diagrams to find potential threats against your system
- Apply Threat Modeling frameworks
- Identify system weaknesses

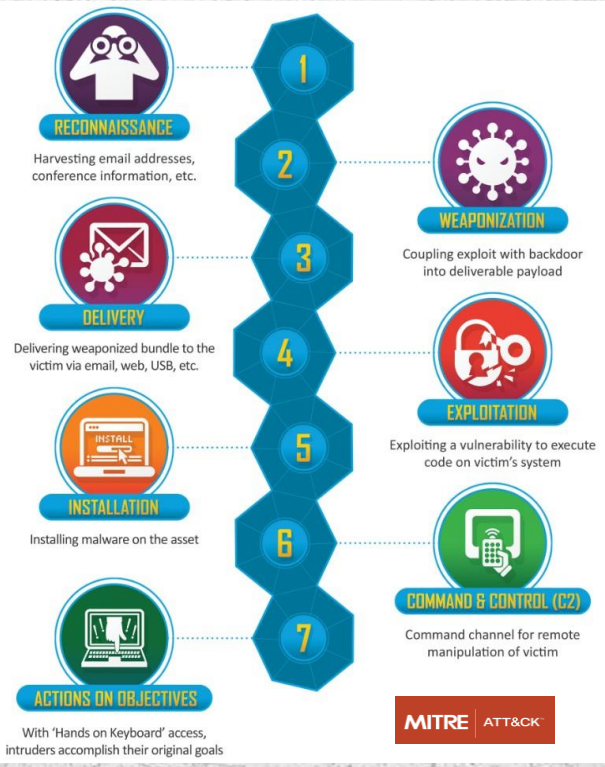


https://www.eccouncil.org/threat-modeling/

COMMON FRAMEWORKS

STRIDE THREAT MODEL

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Pretending to be something or someone other than yourself
T	Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere.
R	Repudiation	Non- Repudiation	Claiming that you didn't do something or we're not responsible. Can be honest or false
I	Information Disclosure	Confidentiality	Providing information to someone not authorized to access it.
D	Denial of service	Availability	Exhausting resources needed to provide service.
E	Elevation of Privilege	Authorization	Allowing someone to do something they are not authorized to do.



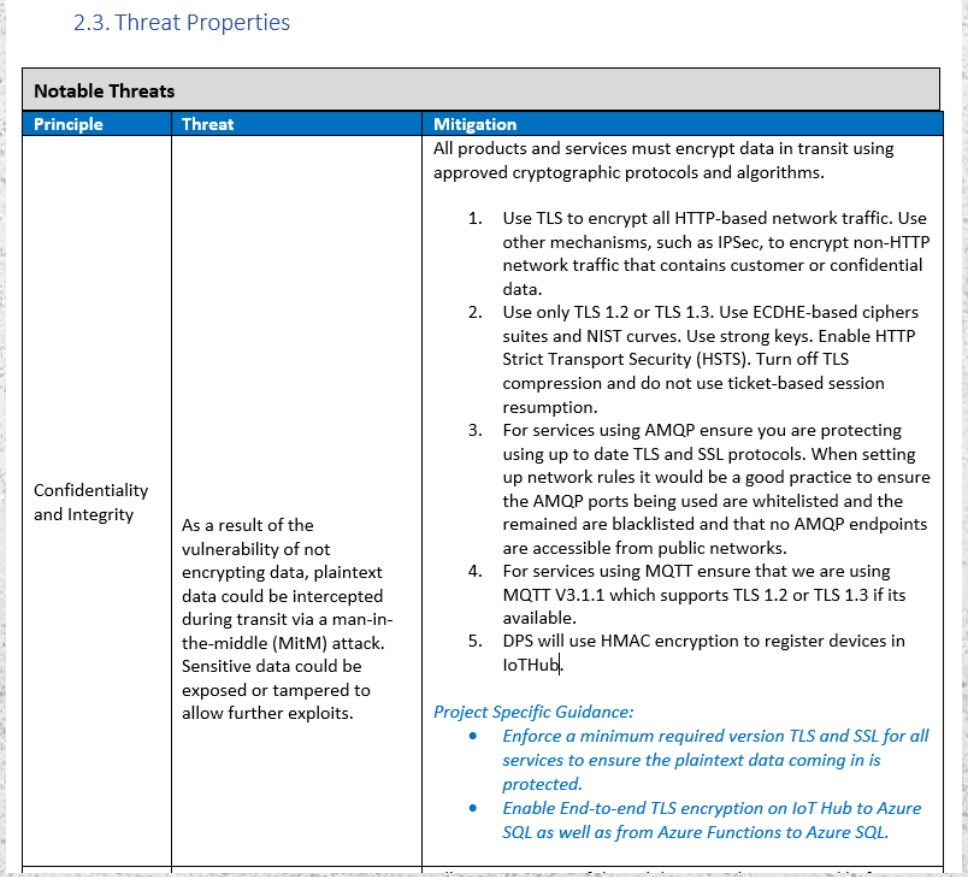
STRIDE MAPPING FOR DFDS

Element	S	T	R	I	D	E
 External entity	✓		✓			
 Process	✓	✓	✓	✓	✓	✓
 Data Store		✓	✓	✓	✓	
 Data Flow		✓		✓	✓	

4 – CREATE MITIGATION STRATEGIES

Goals

- Measure each threat against a prioritization framework or security bug bar
- Track each threat as a task or work item in a backlog
- Generate security control recommendations that are mapped to a threat modeling framework
- Select one or more security control types and functions to address each threat



2.3. Threat Properties

Notable Threats

Principle	Threat	Mitigation
Confidentiality and Integrity	As a result of the vulnerability of not encrypting data, plaintext data could be intercepted during transit via a man-in-the-middle (MitM) attack. Sensitive data could be exposed or tampered to allow further exploits.	All products and services must encrypt data in transit using approved cryptographic protocols and algorithms. 1. Use TLS to encrypt all HTTP-based network traffic. Use other mechanisms, such as IPSec, to encrypt non-HTTP network traffic that contains customer or confidential data. 2. Use only TLS 1.2 or TLS 1.3. Use ECDHE-based ciphers suites and NIST curves. Use strong keys. Enable HTTP Strict Transport Security (HSTS). Turn off TLS compression and do not use ticket-based session resumption. 3. For services using AMQP ensure you are protecting using up to date TLS and SSL protocols. When setting up network rules it would be a good practice to ensure the AMQP ports being used are whitelisted and the remained are blacklisted and that no AMQP endpoints are accessible from public networks. 4. For services using MQTT ensure that we are using MQTT V3.1.1 which supports TLS 1.2 or TLS 1.3 if its available. 5. DPS will use HMAC encryption to register devices in IoTHub. *Project Specific Guidance:* • *Enforce a minimum required version TLS and SSL for all services to ensure the plaintext data coming in is protected.* • *Enable End-to-end TLS encryption on IoT Hub to Azure SQL as well as from Azure Functions to Azure SQL.*

5 – CONTINUOUSLY ITERATE AND VERIFY

Goals

- Confirm all previous and new security requirements are satisfied for the system
- Configure cloud providers, operating systems, and components to meet security requirements
- Ensure all issues are addressed with the right security controls
- Take system through manual and automated verification before deployment

SECURITY STRATEGY

Continuously Verify

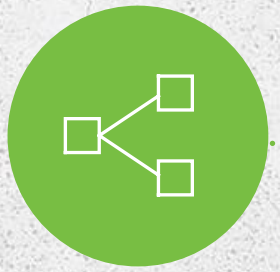
Identify

Identify Security Stakeholders

Evaluate

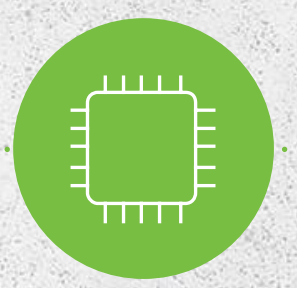
Evaluate Customer Requirements & Architecture

Generate



Generate Data Flow Diagrams for User and Machine Flows

Mitigate



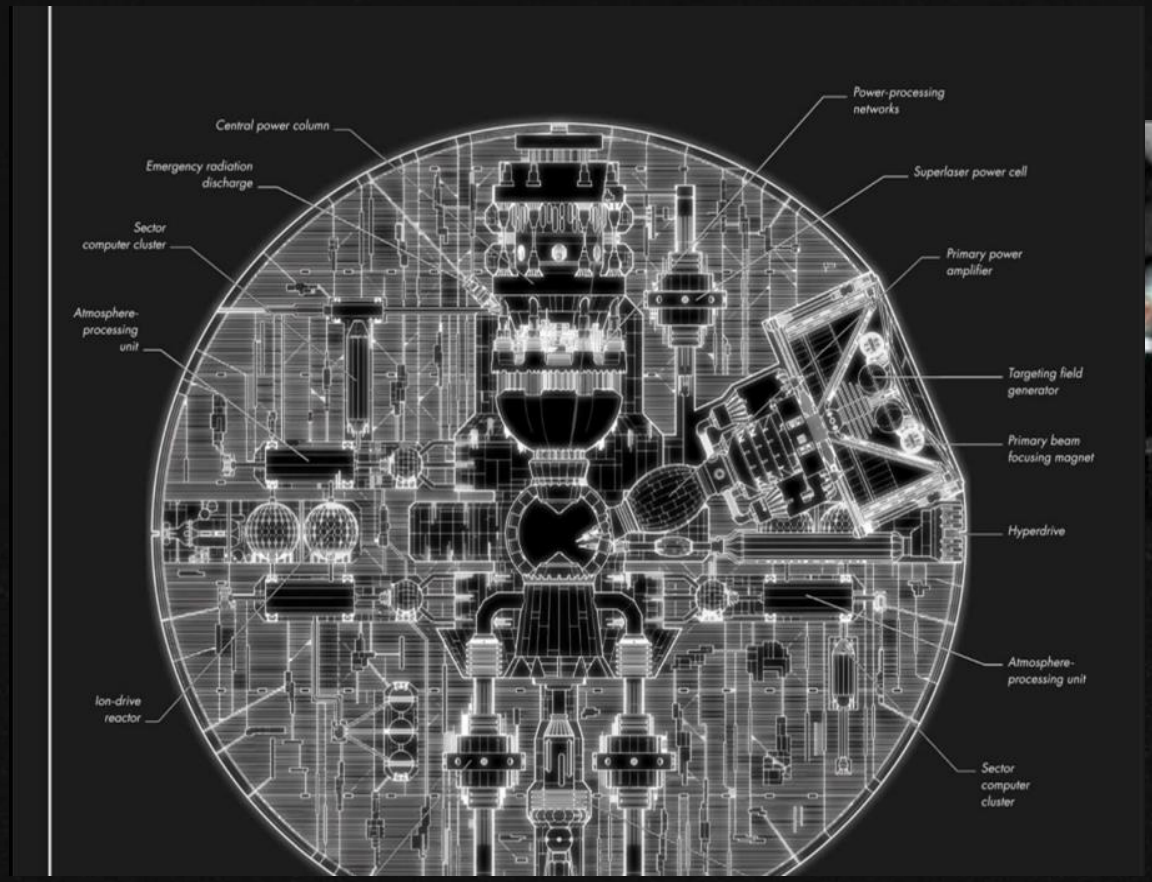
Generate Threat Model Mitigation Strategies with Frameworks

Create

Create Security Backlog Items from Threat Model Mitigations

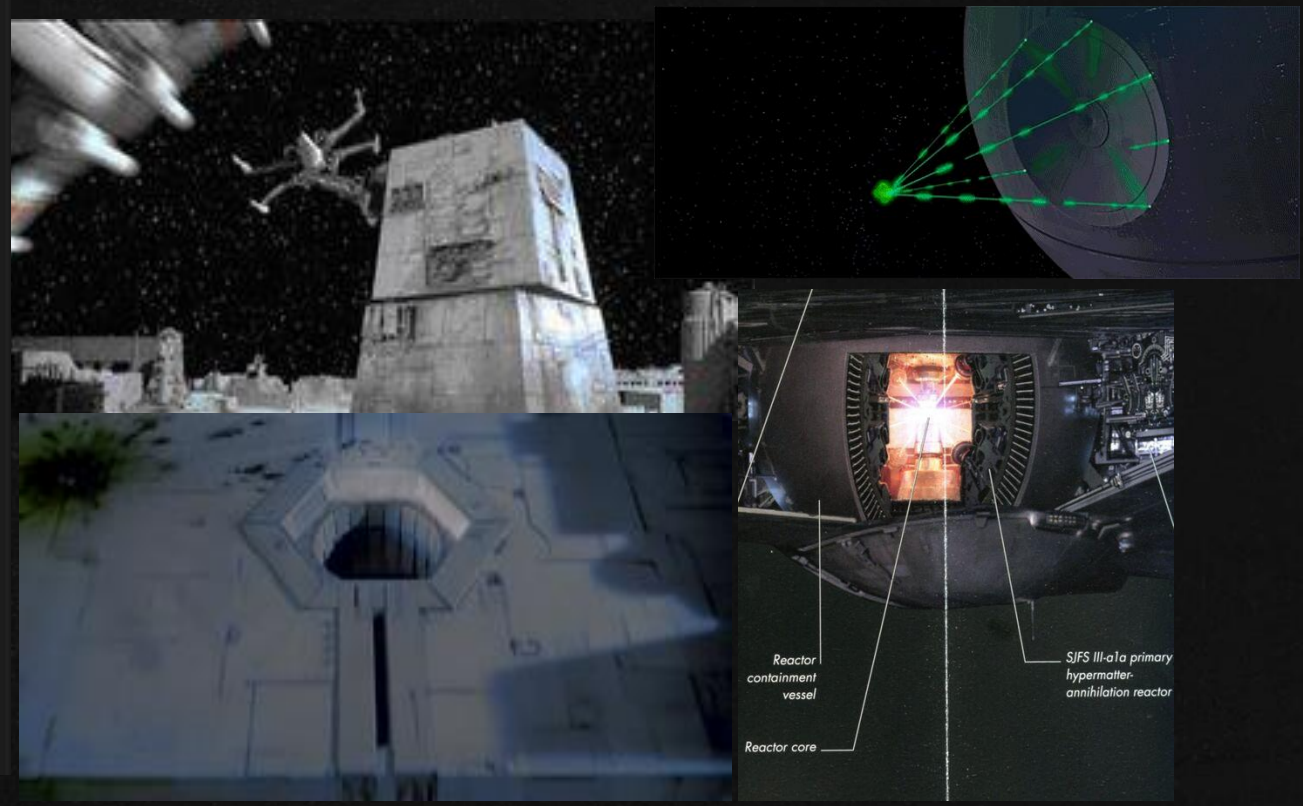
YOU CAN THREAT MODEL ANYTHING!

1 – ANALYZE THE SYSTEM



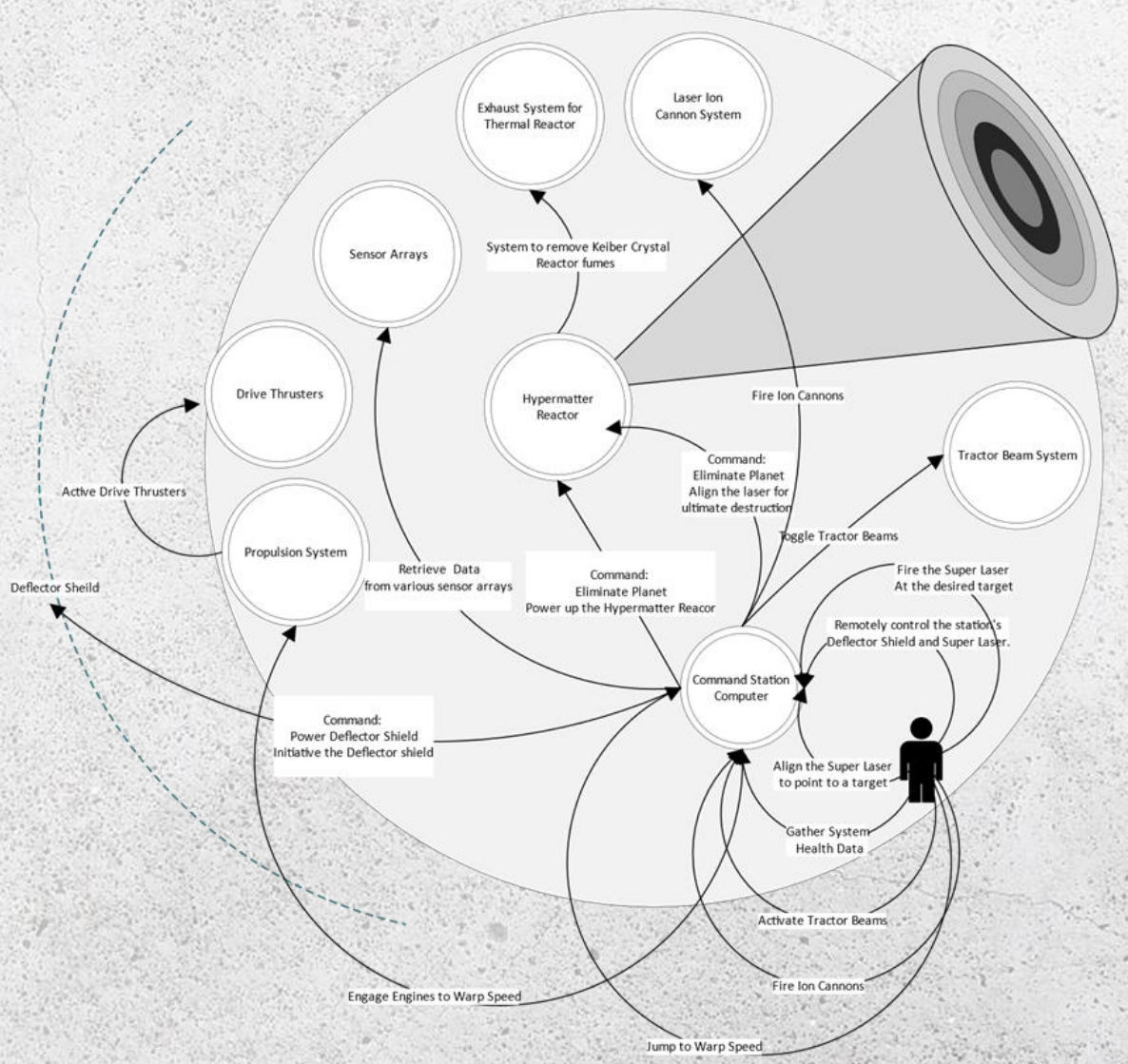
Death Star Mobile Battle Station

DS-1 Orbital Battle Station

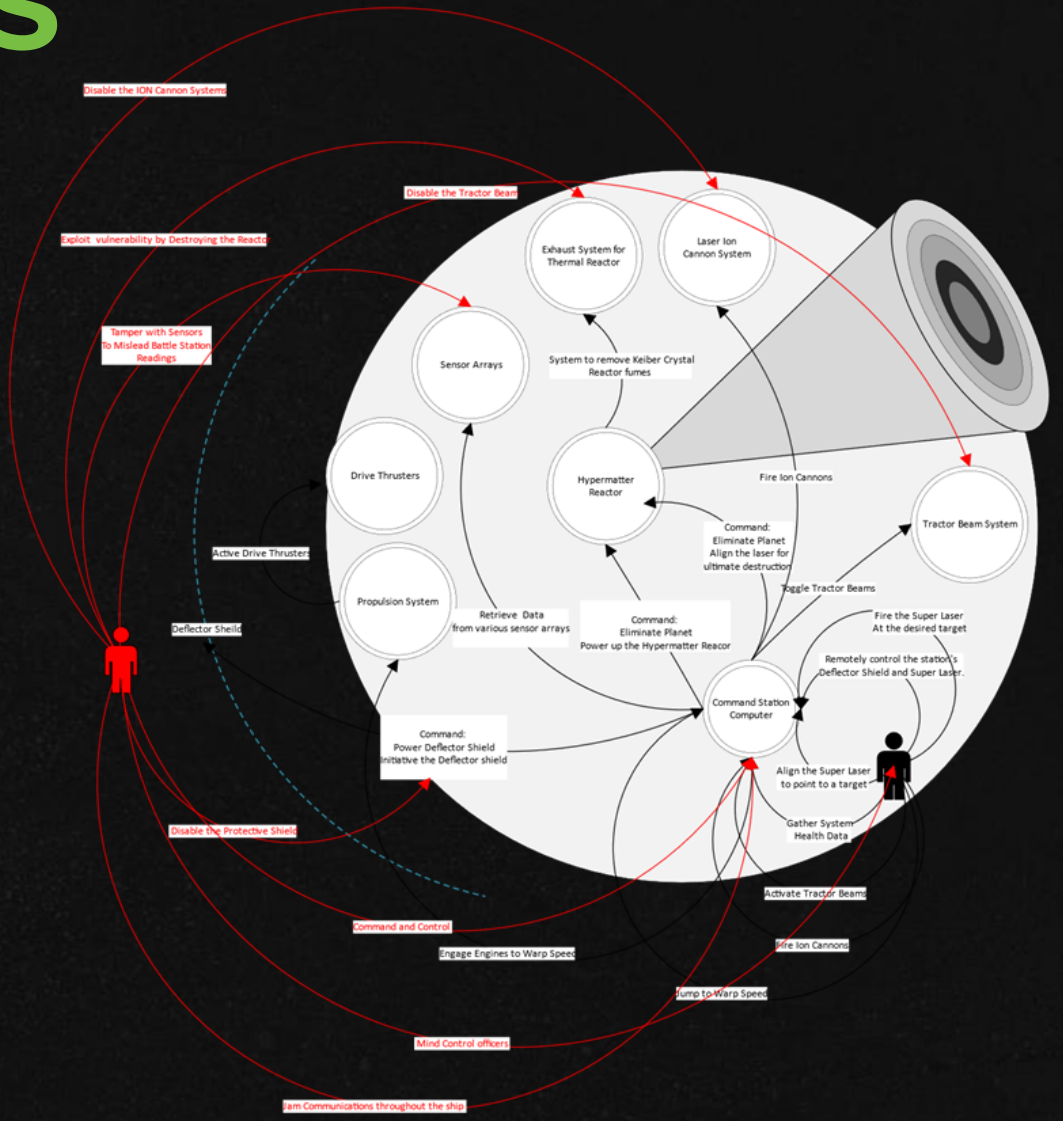


How the Death Star Works

2 – DESIGN A DATAFLOW DIAGRAM



3 – IDENTIFY THREATS



4 – CREATE MITIGATION STRATEGIES

Vulnerability	Thermal Exhaust Port
Action	Exploitation
Definition	**exploit** means to take advantage of a vulnerability
Example	Luke Skywalker exploiting the thermal exhaust vent by launching torpedoes into the vent, impacting the core and triggering a catastrophic explosion
Mitigation	Eliminate the two-meter-wide thermal exhaust port, or safeguard this exhaust vent with extra defenses and perimeters

SPOOFING

https://www.youtube.com/watch?v=Y3VQpg04vXo

Threat	Spoofing
Property	Authentication
Definition	Spoofing threats involve an adversary creating and exploiting confusion about who's talking to whom
Example	Impersonate storm troopers to hijack communication systems and save princesses as done so by Han Solo and Luke Skywalker
Mitigation	Authenticate principals (users or machines) by enabling more robust & multiple identity mechanisms such as MFA

TAMPERING

Threat	Tampering
Property	Integrity
Definition	Tampering threats involve an adversary modifying data, usually as it flows across a network, in memory, on disk or in databases
Example	Obi-Wan Kenobi Tampering with the tractor beam system to allow the Millennium Flacon to fly into the sunset
Mitigation	Add validation (credentials, codes) and safeguards (cameras, guards, limited access) around the machinery

REPUDIATION

Threat	Repudiation
Property	Non-Repudiation
Definition	Repudiation threats involve an adversary denying that something happened or claiming to have not performed an action
Example	Han Solo saying “there's a very dangerous reactor meltdown" in attempt to staging a divergence
Mitigation	Ensuring proper observability is in place to track down adversarial behaviors and logging behaviors

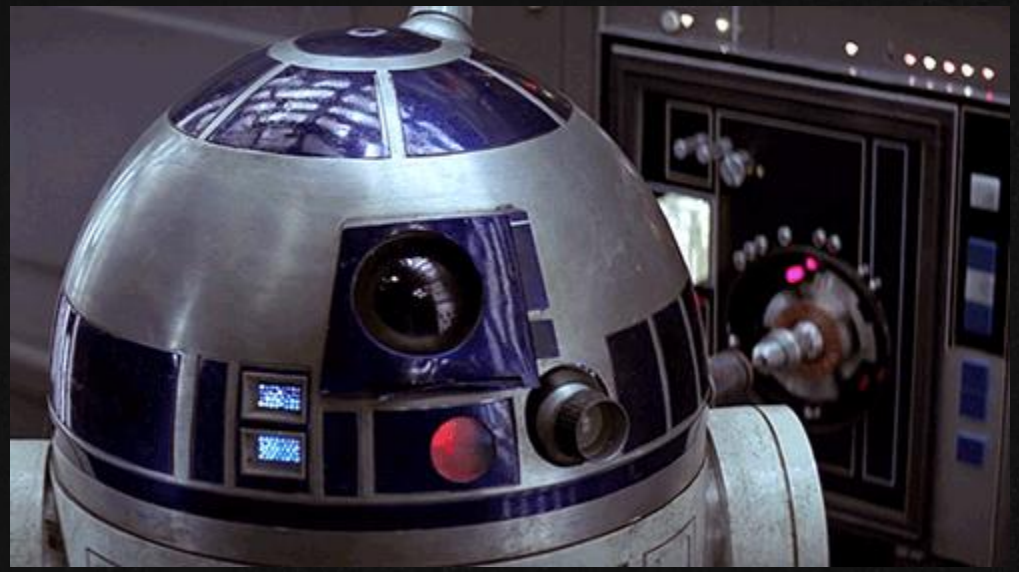
INFORMATION DISCLOSURE

Threat	Information Disclosure
Property	Confidentiality
Definition	Exposing information to someone not authorized to see it
Example	Jyn Erso relaying critical death star vulnerability information to the rebel alliance
Mitigation	A thorough understanding of your asset inventory, and public exposure are also highly important to help with mitigation for this threat

DENIAL OF SERVICE

Threat	Denial of Service
Property	Availability
Definition	Deny or degrade service to users
Example	Chewie jamming transmission channels for a tie fighter
Mitigation	Ensuring communication channels are encrypted and only verified users can access these channels. Also practicing redundancy, such as a backup channel available

ESCALATION OF PRIVILEGES



Threat	Privilege Escalation
Property	Authorization
Definition	Elevation of privilege threats involve an adversary being able to do something, or obtain the rights to do things, which they have not been authorized to do
Example	R2D2 Hacking into the death star system to open doors and extract information. Jedi mind controls “These are not the droids you're looking for”
Mitigation	Put checks in place to verify appropriate access levels with each request

5 – CONTINUOUSLY ITERATE AND VERIFY

LEARNING MATERIALS

Microsoft Security Development Lifecycle

Microsoft Security Development Lifecycle

Microsoft Learn – Threat Modeling

Threat Modeling Security Fundamentals - Training | Microsoft Learn

The OWASP Top Ten

https://owasp.org/www-project-top-ten/

MITRE ATT&CK

https://attack.mitre.org/

STRIDE

https://en.wikipedia.org/wiki/STRIDE_%28security%29

Security Framework overviews

https://docs.google.com/document/d/1nBMKvN5qti5EkV_QtjsX-kGMI8rnNj05BEZFNrx2x4o/edit#heading=h.ndpja5lhlgd8

NIST Guidance for Data Centric Threat Models

https://csrc.nist.gov/CSRC/media/Publications/sp/800-154/draft/documents/sp800_154_draft.pdf

Thank You to Our Sponsors and Hosts!

AppSec NZ
appsec.org.nz

OWASP NEW ZEALAND
owasp.org.nz

AUT UNIVERSITY
TE WĀNANGA ARONUI O TAMAKI MAKAU RAU

BASTION
SECURITY GROUP

DATACOM

aws

84.

PentesterLab

plexure

VERACODE

Without them, this Conference couldn't happen.


THANK YOU!
MAY THE FORCE BE WITH US.