Threat Modelling

INTRODUCTION

MANISH SHARMA

WORKING AT Gainsight

FOLLOW/CONNECT ME @

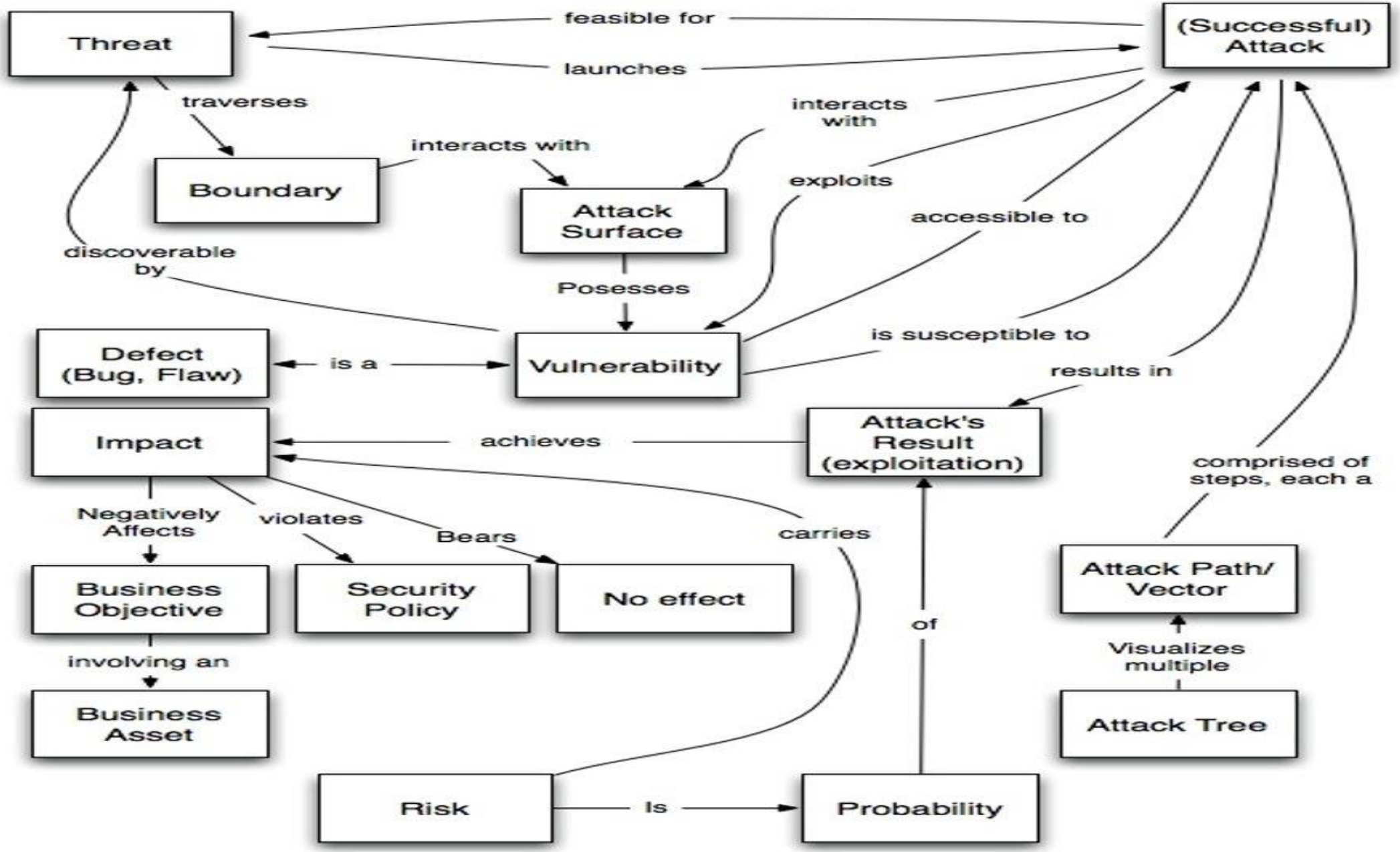
LINKEDIN/sh377c0d3

TWITTER: @sh377c0d3

GITHUB/sh377c0d3

AGENDA

- What is Threat Modelling?
- How does it work?
- Threat Modelling Frameworks
- Conduct a Threat Analysis
- How to conduct threat modelling?
- Pros and Cons
- Best Practices and Brain Storming


Threat
feasible for
(Successful) Attack
launches
traverses
interacts with
Boundary
interacts with
Attack Surface
exploits
accessible to
discoverable by
Posesses
Defect (Bug, Flaw)
is a
Vulnerability
is susceptible to
results in
Impact
achieves
Attack's Result (exploitation)
comprised of steps, each a
Negatively Affects
violates
Bears
carries
Business Objective
Security Policy
No effect
Attack Path/ Vector
of
Visualizes multiple
involving an
Business Asset
Attack Tree
Risk
Is
Probability

WHAT IS THREAT MODELLING?

- It's Structured Process
- First thing first : **Bring me the diagram**
- **Range includes Network, Application, System, Distributed System, IoT devices, Business process and more.**
- Capturing, Organizing and Analyzing

1. Define Objectives	• Identify Business Objectives • Identify Security and Compliance Requirements • Business Impact Analysis
2. Define Technical Scope	• Capture the Boundaries of the Technical Environment • Capture Infrastructure | Application | Software Dependencies
3. Application Decomposition	• Identify Use Cases | Define App. Entry Points & Trust Levels • Identify Actors | Assets | Services | Roles | Data Sources • Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis	• Probabilistic Attack Scenarios Analysis • Regression Analysis on Security Events • Threat Intelligence Correlation and Analytics
5. Vulnerability & Weaknesses Analysis	• Queries of Existing Vulnerability Reports & Issues Tracking • Threat to Existing Vulnerability Mapping Using Threat Trees • Design Flaw Analysis Using Use and Abuse Cases • Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling	• Attack Surface Analysis • Attack Tree Development | Attack Library Mgt. • Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis	• Qualify & Quantify Business Impact • Countermeasure Identification and Residual Risk Analysis • ID Risk Mitigation Strategies

WHAT IS THREAT MODELLING? (CONTD..)

- Objectives:
  - Identify Security Requirements
  - Pinpoint Security Threats
  - Potential Vulnerability
  - Prioritize Remediation

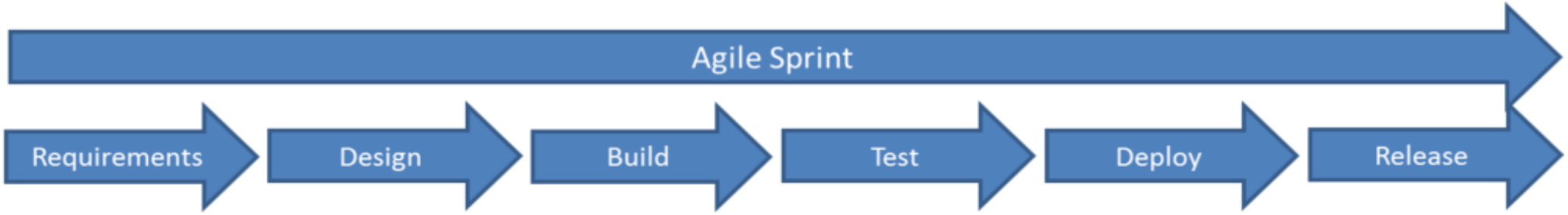
- Four Question Framework:
  - What are we working on?
  - What can go wrong?
  - What are we going to do about it?
  - Did we do a good job?

QUICK SUMMARIZE !

- Hunt Threats ahead i.e, at the time of Development

- Catch - Need to have right Security Mind-set

WE NEED SECURITY !



	Requirements	Design	Build	Test	Deploy	Release
SwA	- Modeling - Derived Req. - Security Req.	- Secure Design -Architectural Analysis	-Origin Analysis - Code Review - Static Analysis - Unit Test - Formal Methods	-Dynamic Analysis - Penetration Testing	- Regression & Performance testing - Automation - Red Teaming	- Vulnerability tracking - Operational monitoring
Agile	- Sprint Planning - Definition of Ready	- Refactoring	- Continuous Integration - Configuration Management - IDE	- Test Automation	- Automated Deployment - Sprint Demo - User Testing	- Release Management

Figure 1: SDLC with Software Assurance and Agile Development Process Overlays

HOW DOES IT WORK?

- Let's Recall everything that we discussed in our Previous slide
- Steps:

1. **Bring me the diagram**: What we are building?
2. **Identify threats**: What could go wrong?
3. **Mitigating**: What we are doing to defend against the Threat?
4. **Validating**: Have we acted on each previous steps:?

THREAT MODELLING FRAMEWORKS

STRIDE

PASTA

DREAD

Attack Trees

CVSS

hTMM

Total Frameworks = 12

STRIDE

- Used to Identify the Threats
- Created by Engineers at Microsoft
- Guide the discover of threat within system
- Used along with Model of the Target System
- Most Effective for Evaluating Individual System

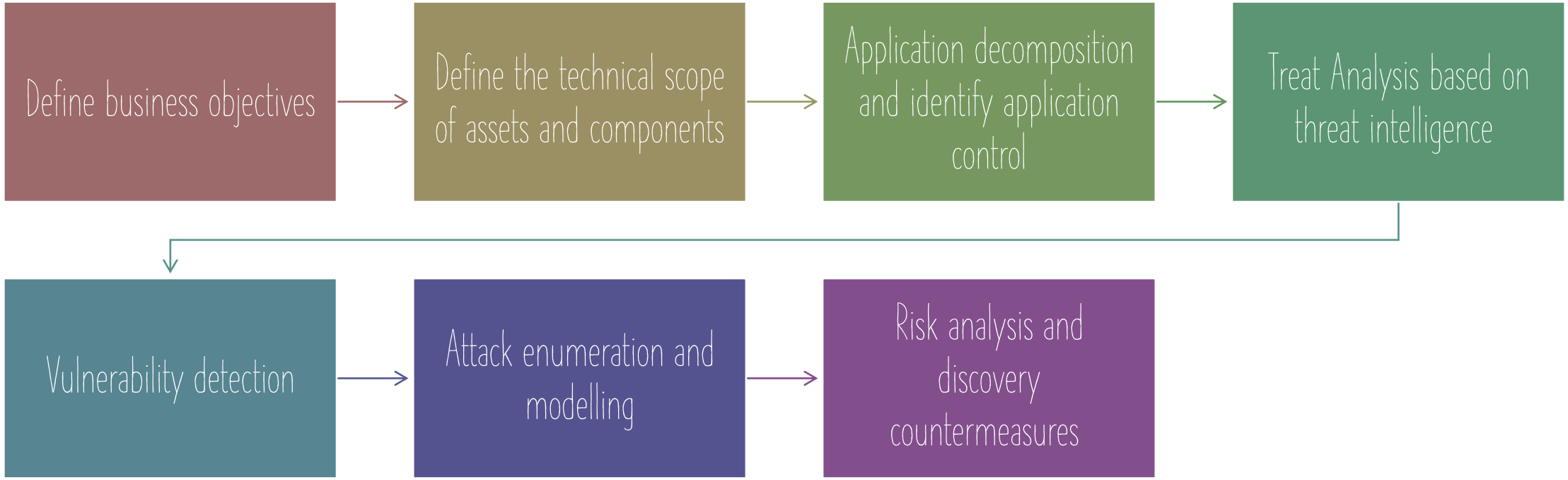
STRIDE (CONTD..)

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

PASTA

- **P**rocess for **A**ttack **S**imulation and **T**hreat **A**nalysis
- Attack Centric Methodology
- Consists of 7 steps
- Designed to correlate business objectives with technical requirements
- Dynamically identity, count and prioritize threat

PASTA (CONTD..)


Define business objectives
Define the technical scope of assets and components
Application decomposition and identify application control
Treat Analysis based on threat intelligence
Vulnerability detection
Attack enumeration and modelling
Risk analysis and discovery countermeasures

DREAD

- More focused on "Risk Analysis" and less on the "Threat Actor"
- DREAD stands for six questions you would ask about each potential threat:
  - Damage potential: How great is the damage if the vulnerability is exploited?
  - Reproducibility: How easy is it to reproduce the attack?
  - Exploitability: How easy is it to launch an attack?
  - Affected users: As a rough percentage, how many users are affected?
  - Discoverability: How easy is it to find the vulnerability?
- Each of these questions is answered with a rating between one and three.

STRIDE or PASTA or DREAD

- DREAD was conceived of as an add-on to the STRIDE model that allows modellers to rank threats once they've been identified.

- Use STRIDE to Identify the Threats & then use DREAD to evaluate Risk Associated with those Threats

- PASTA - Is it Attacker Centric or Risk Centric ? Well.. This debate is like Windows vs Mac which is best...

ATTACK TREE

- Attack trees are charts that display the paths that attacks can take in a system.
- These charts display attack goals as a root with possible paths as branches.
- When creating trees for threat modeling, multiple trees are created for a single system, one for each attacker goal.
- This is one of the oldest and most widely used threat modeling techniques.
- While once used alone, it is now frequently combined with other methodologies, including PASTA, CVSS, and STRIDE.

CVSS

CVSS v2.0 Ratings	
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

CVSS v3.0 Ratings	
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- Common Vulnerability Scoring System
- It is a standardized threat scoring system used for known vulnerabilities.
- Developed by the National Institute of Standards and Technology (NIST) and maintained by the Forum of Incident Response and Security Teams (FIRST)
- Inherent properties of a threat and the impacts of the risk factor due to time since the vulnerability was first discovered.
- Measures that allow security teams to specifically modify risk scores based on individual system configurations.

HTMM

- Hybrid Threat Modelling Method
- hTMM is a methodology developed by Security Equipment Inc. (SEI) that combines two other methodologies:
  - Security Quality Requirements Engineering (SQUARE)–a methodology designed to elicit, categorize and prioritize security requirements.
  - Persona non Grata (PnG)–a methodology that focuses on uncovering ways a system can be abused to meet an attacker's goals.
- Accounts for all possible threats, produces zero false positives, provides consistent results, and is cost effective.

CONDUCT A THREAT ANALYSIS

- Checklist-based approaches.
- Non-checklist-based approaches. Generally, use creative methods (e.g., brainstorming) to identify attacks.
- Synopsys threat analysis uses a quasi-checklist approach: It uses a template to drive the core analysis but still leaves the opportunity for creative analysis.
- Synopsys uses pre-baked application protocol threat analysis for commonly used application-level protocols, such as OAuth, SAML, OIDC, Kerberos, password-based authentication, and others.
    - This list is not exhaustive, but it allows you to start thinking about areas of concern to analyze.

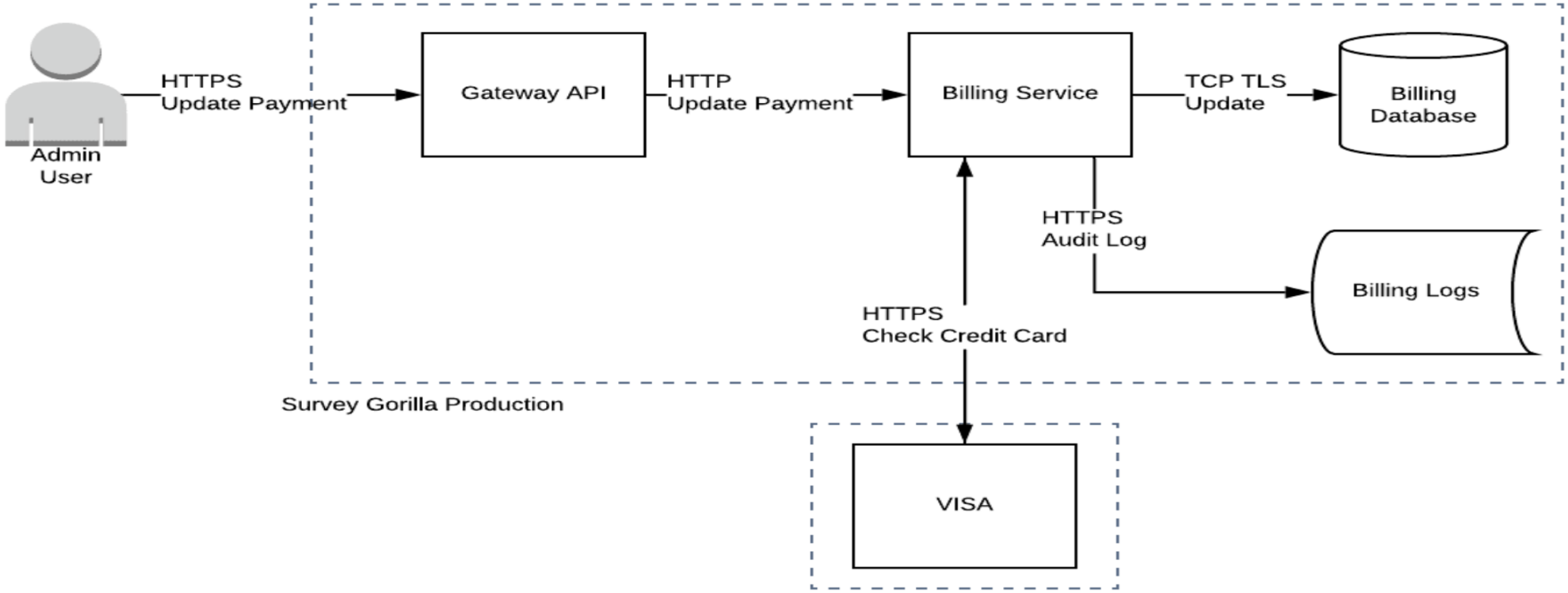
HOW TO CONDUCT THREAT MODELLING?

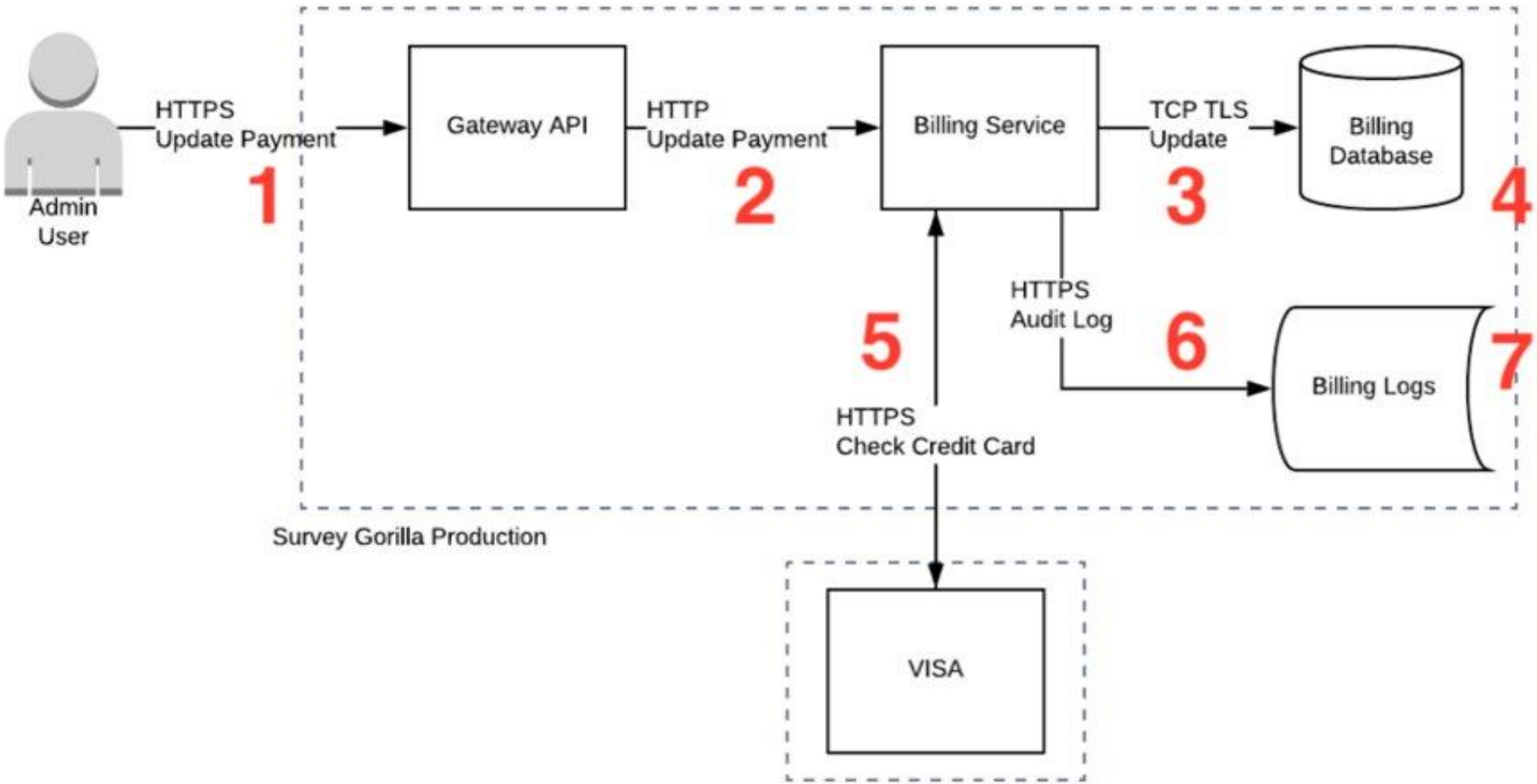
- Let's sit together and start Brain Storming !!!

1. Application
2. Cloud
3. Mobile
4. IoT
5. Network

BRING ME THE DIAGRAM !!!

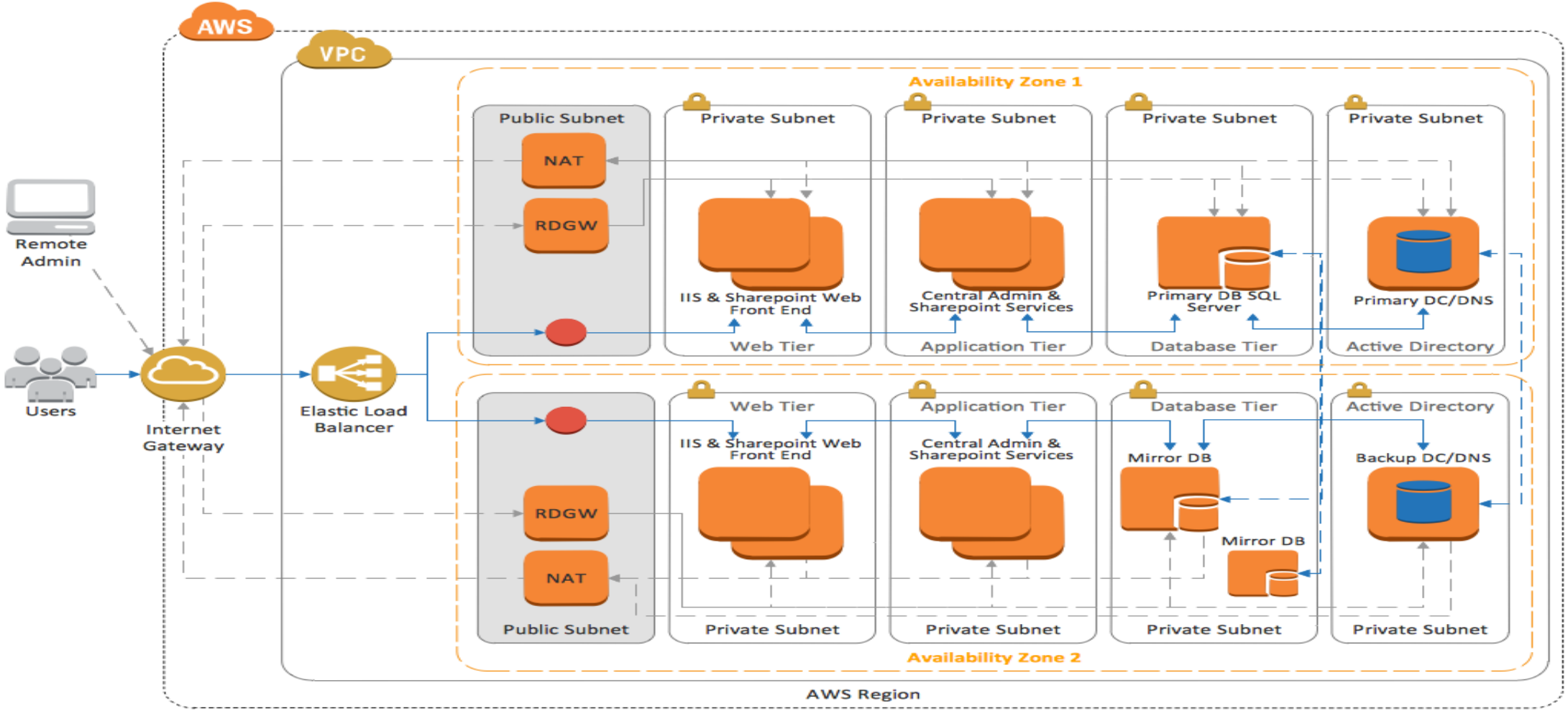
APPLICATION



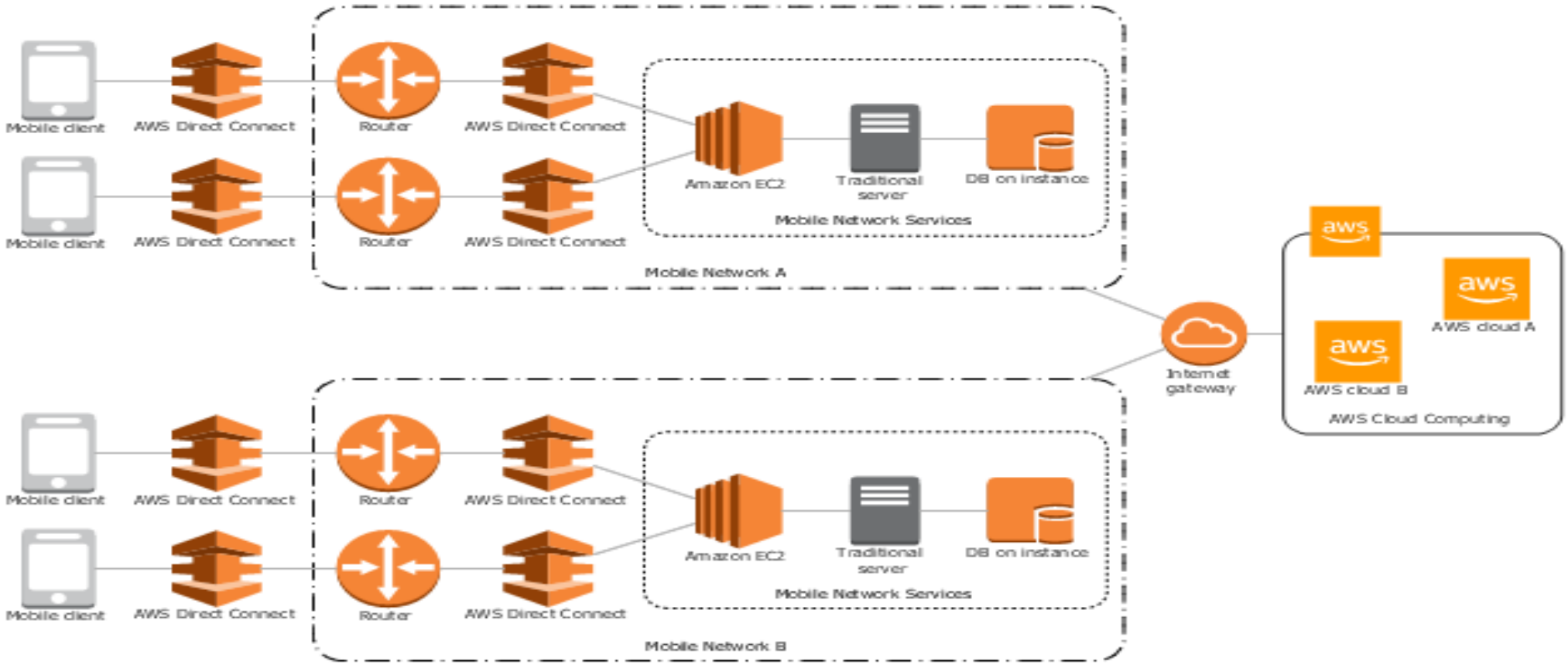

Admin User
HTTPS
Update Payment
1
Gateway API
HTTP
Update Payment
2
Billing Service
TCP TLS
Update
3
Billing Database
4
HTTPS
Audit Log
6
Billing Logs
7
5
HTTPS
Check Credit Card
Survey Gorilla Production
VISA

CLOUD

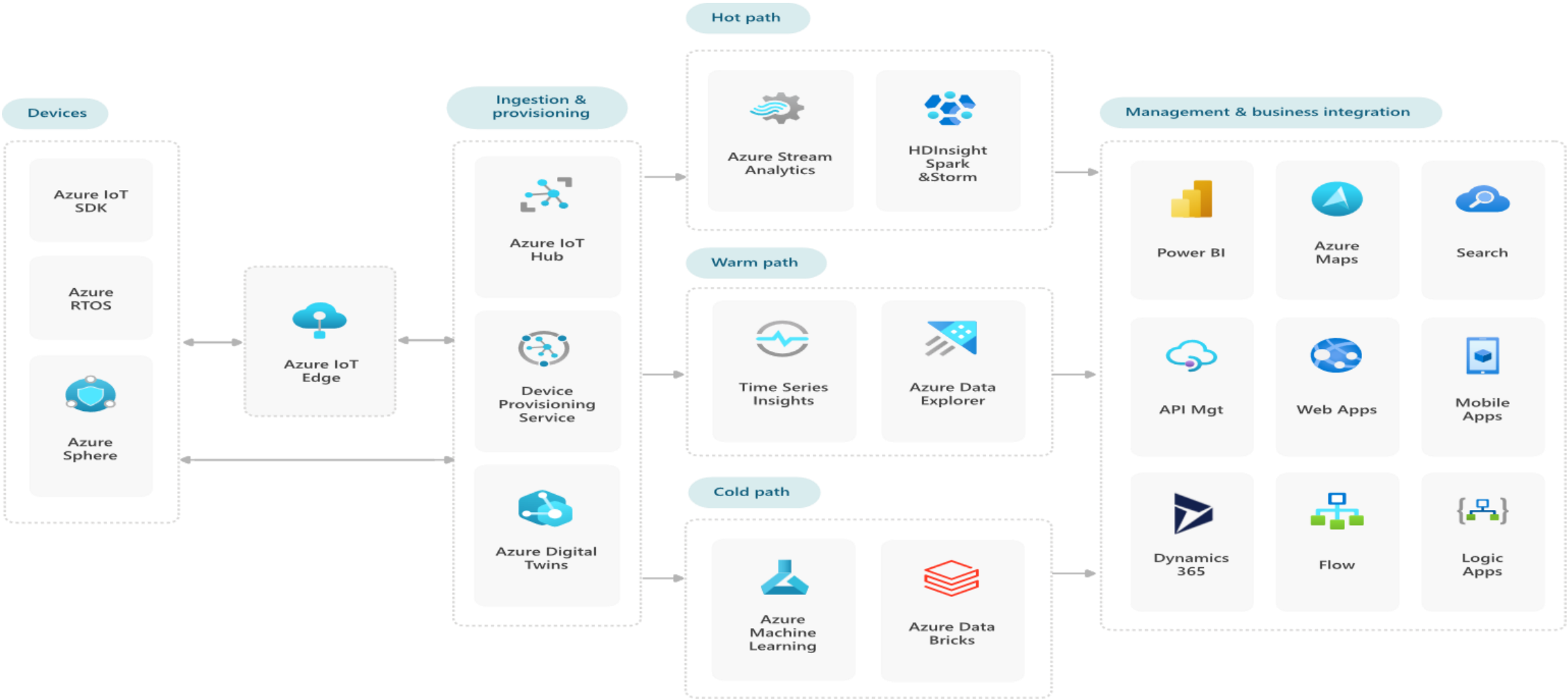
SharePoint server reference architecture for public-facing website scenario



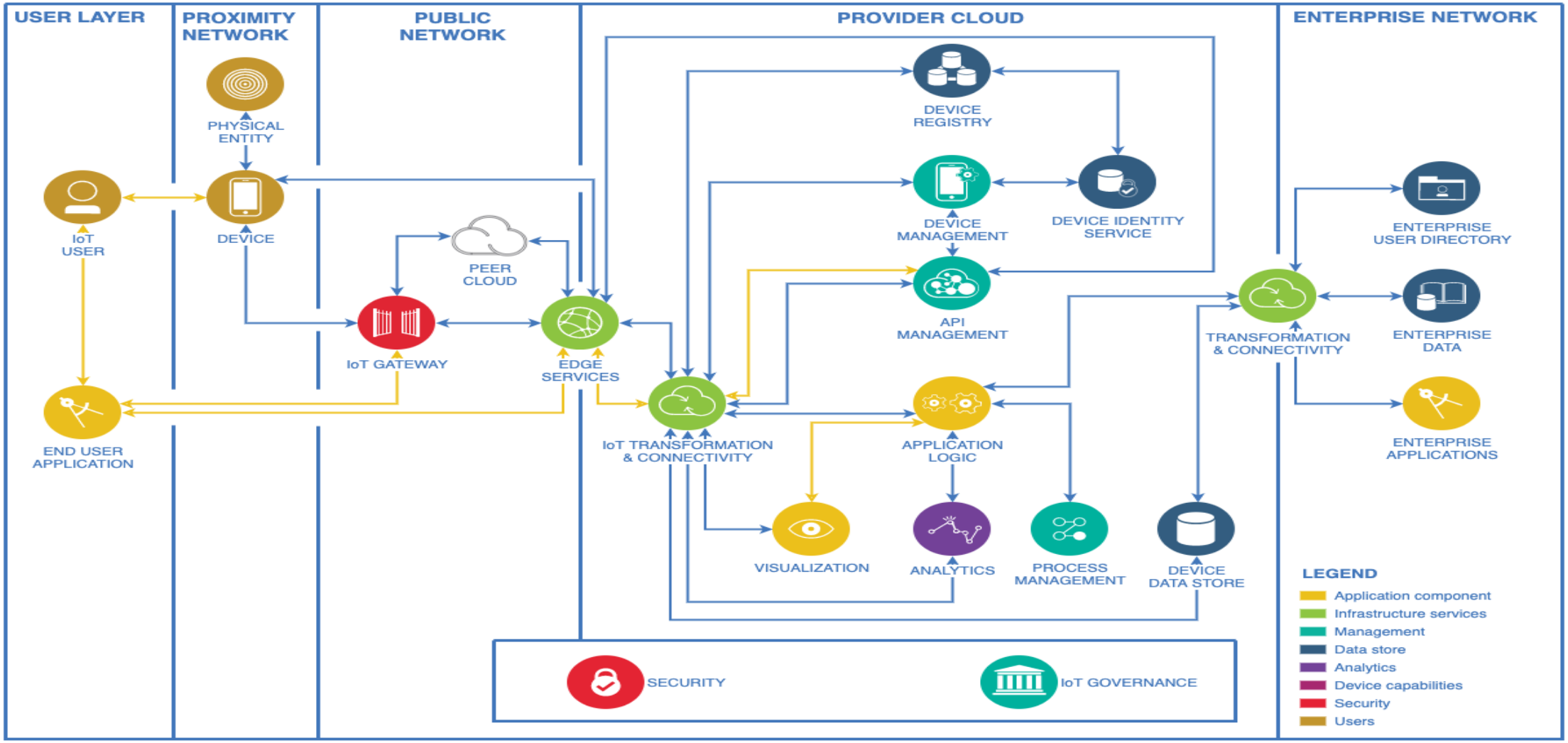
MOBILE


Mobile client
AWS Direct Connect
Router
AWS Direct Connect
Amazon EC2
Traditional server
DB on instance
Mobile Network Services
Mobile Network A
Mobile Network B
Internet gateway
AWS cloud A
AWS cloud B
AWS Cloud Computing

IOT

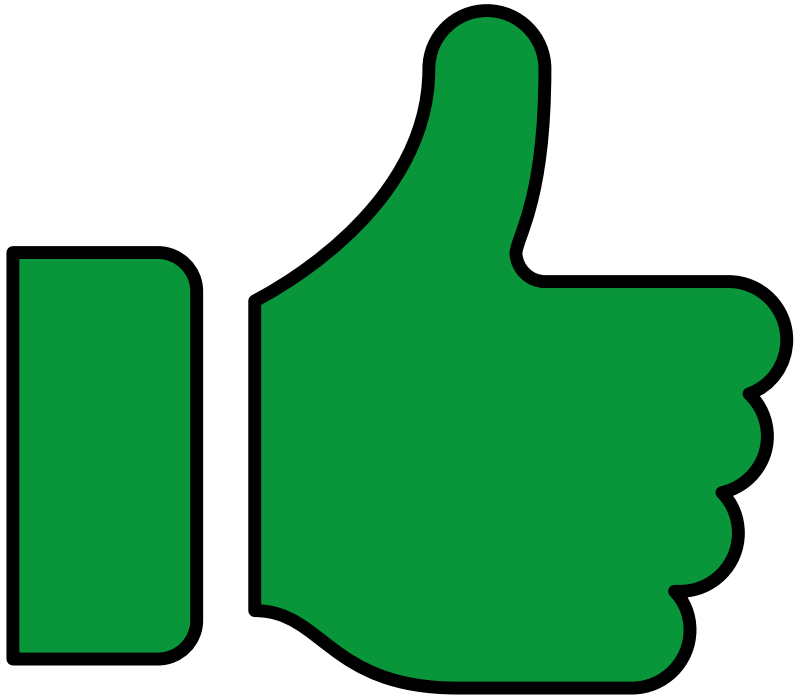

Devices
Azure IoT SDK
Azure RTOS
Azure Sphere
Azure IoT Edge
Ingestion & provisioning
Azure IoT Hub
Device Provisioning Service
Azure Digital Twins
Hot path
Azure Stream Analytics
HDInsight Spark &Storm
Warm path
Time Series Insights
Azure Data Explorer
Cold path
Azure Machine Learning
Azure Data Bricks
Management & business integration
Power BI
Azure Maps
Search
API Mgt
Web Apps
Mobile Apps
Dynamics 365
Flow
Logic Apps

NETWORK


USER LAYER
PROXIMITY NETWORK
PUBLIC NETWORK
PROVIDER CLOUD
ENTERPRISE NETWORK
PHYSICAL ENTITY
IoT USER
DEVICE
PEER CLOUD
IoT GATEWAY
EDGE SERVICES
END USER APPLICATION
DEVICE REGISTRY
DEVICE MANAGEMENT
DEVICE IDENTITY SERVICE
API MANAGEMENT
IoT TRANSFORMATION & CONNECTIVITY
APPLICATION LOGIC
VISUALIZATION
ANALYTICS
PROCESS MANAGEMENT
DEVICE DATA STORE
TRANSFORMATION & CONNECTIVITY
ENTERPRISE USER DIRECTORY
ENTERPRISE DATA
ENTERPRISE APPLICATIONS
SECURITY
IoT GOVERNANCE
LEGEND
Application component
Infrastructure services
Management
Data store
Analytics
Device capabilities
Security
Users

PROS

- Reduce attack Surface
- Prioritize Threat
- Mitigating efforts
- Identify and Eliminate single point of failure
- Understand the complete cyberattack kill chain
- Improve security posture
- Prioritize development and testing efforts



CONS

- Long run and Mystify
- Process gets long and complex
- Disconnected from the development process
- Did we get all threats?
- When to stop finding threats?
- Tracking

BEST PRACTICES AND BRAIN STORMING

Well... Every Security Professional/Organization have their own requirements & Standards.

Can't we have our own Framework to follow? Or Can't we merge more than 2 Framework? .... Of course, we can!

Why don't we use OWASP Based Threat Modelling Approach

Combine Threat Modelling Framework and make use of more than 2 as per your need.

BEST PRACTICES AND BRAIN STORMING (CONTD.)

Don't forget basic building blocks

- Infosec Policy
- Security Standards
- Security Controls

Don't Forget to Research & Analyze OWASP Threat Modelling Approach

Keep on researching and improving Security Posture

At the end of the Day, we are Human Being

Why don't we question ourself on Relevance

THANK YOU