RSAConference2018
San Francisco | April 16–20 | Moscone Center

SESSION ID: DEV-R04

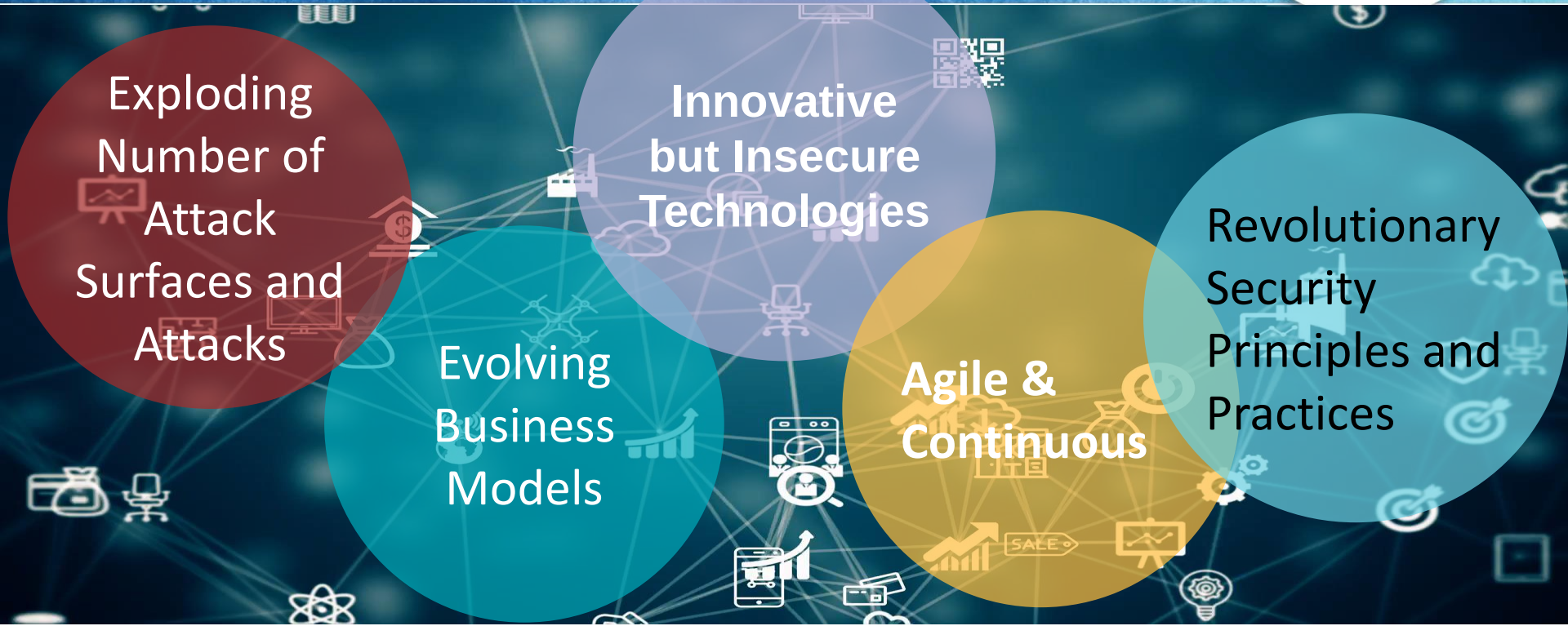
AGILE AND CONTINUOUS THREAT MODELS

Nancy Davoust

Vice President, Security Architecture and Technology Solutions
Comcast

CONTEXT FOR AGILE AND CONTINUOUS THREAT MODELING

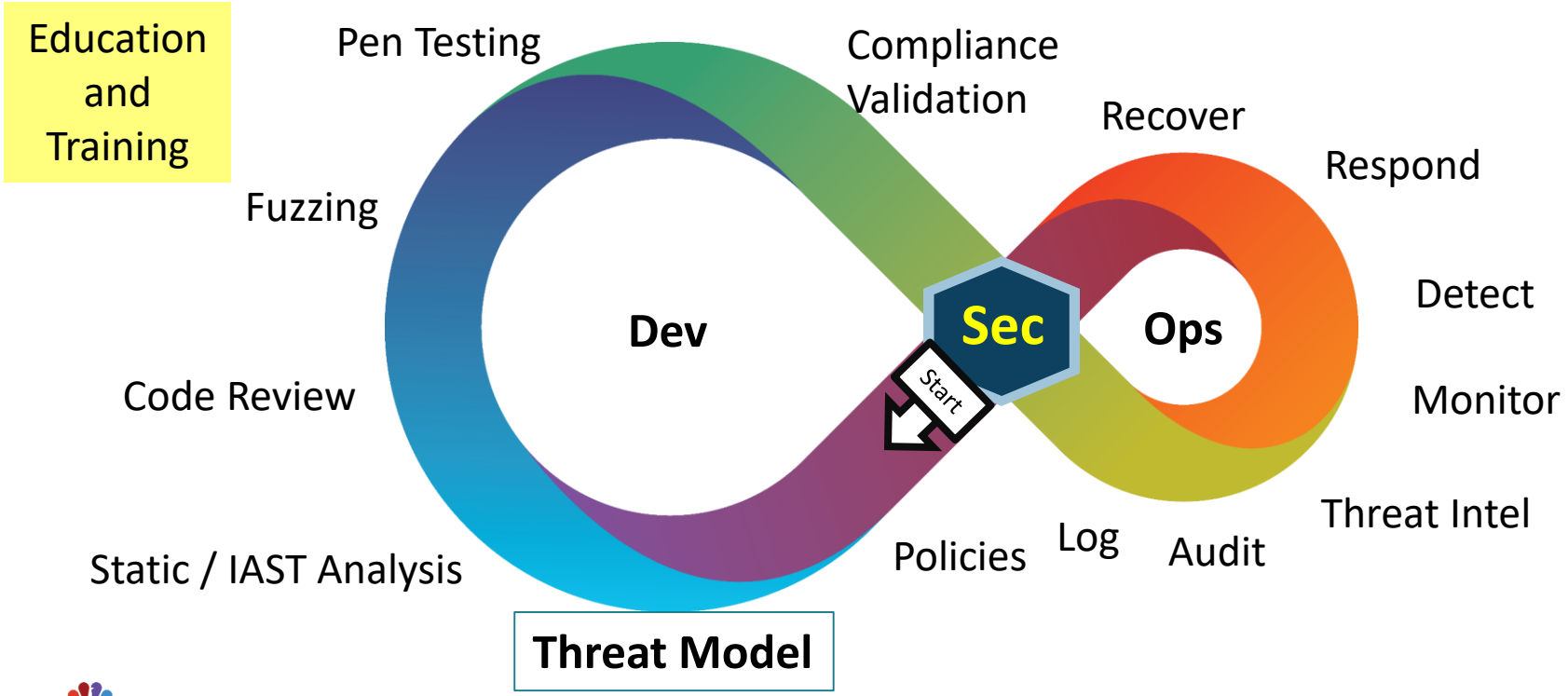
The Landscape is Chaotic



Embracing Agile and Continuous Methodology

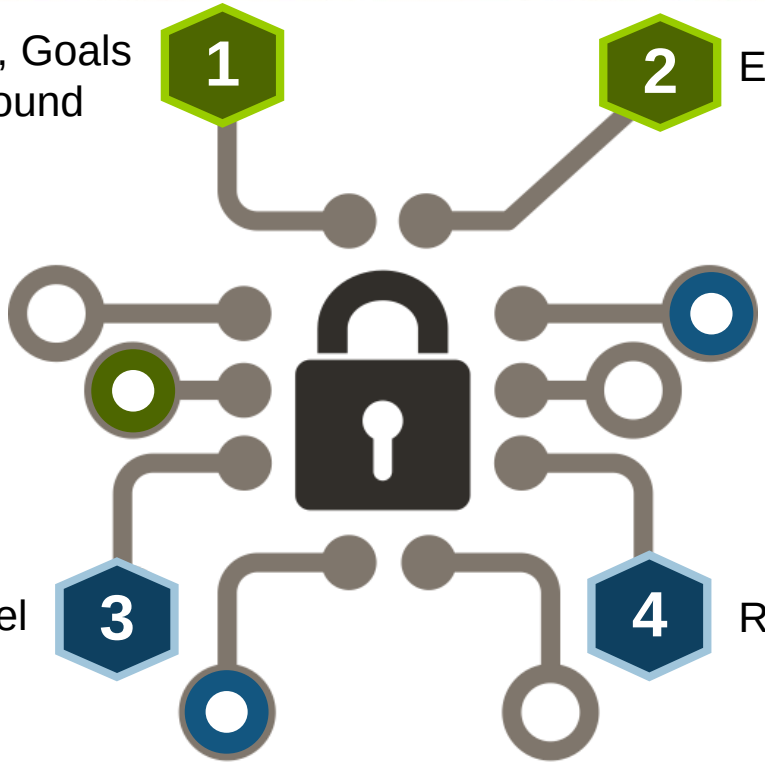
While we are Developing and Operating at the Speed of Light

Build Security In – Don't Bolt It On



AGILE AND CONTINUOUS THREAT MODEL WORKSHOP

Threat Model Workshop In a Day with Each DevSecOps Team



Introduction, Goals and Background

Examples and Exercises

Live Threat Model

Risk Assessment

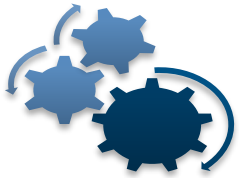
Threat Modeling Workshop Success Objectives

- Team trained to use agile and continuous threat modeling as a practice
- Reviewed architecture for real-world threats
- Common understanding of the threats and mitigations
- Protect customers and products earlier in the product lifecycle
- Team buy-in as the security findings were generated by the team

Everyone is Responsible for Security

- Open Posture
- Transparent
- One Team

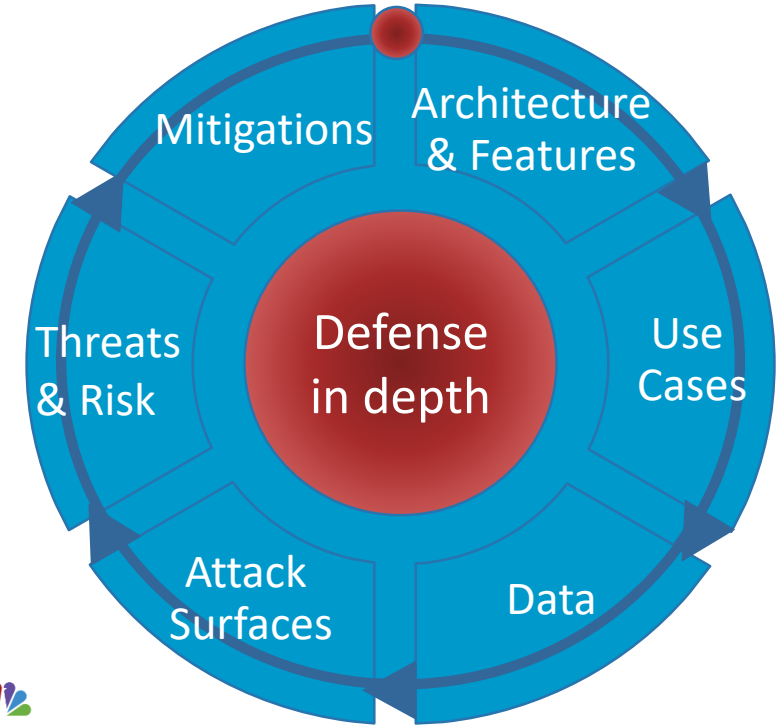
- Be Honest
- No Blaming
- We are here to help one another



- Build security in by design
- Teamwork to identify attack surfaces
- We are all in this together

Threat Modeling Fundamentals

What is threat modeling?



Why do we need it?

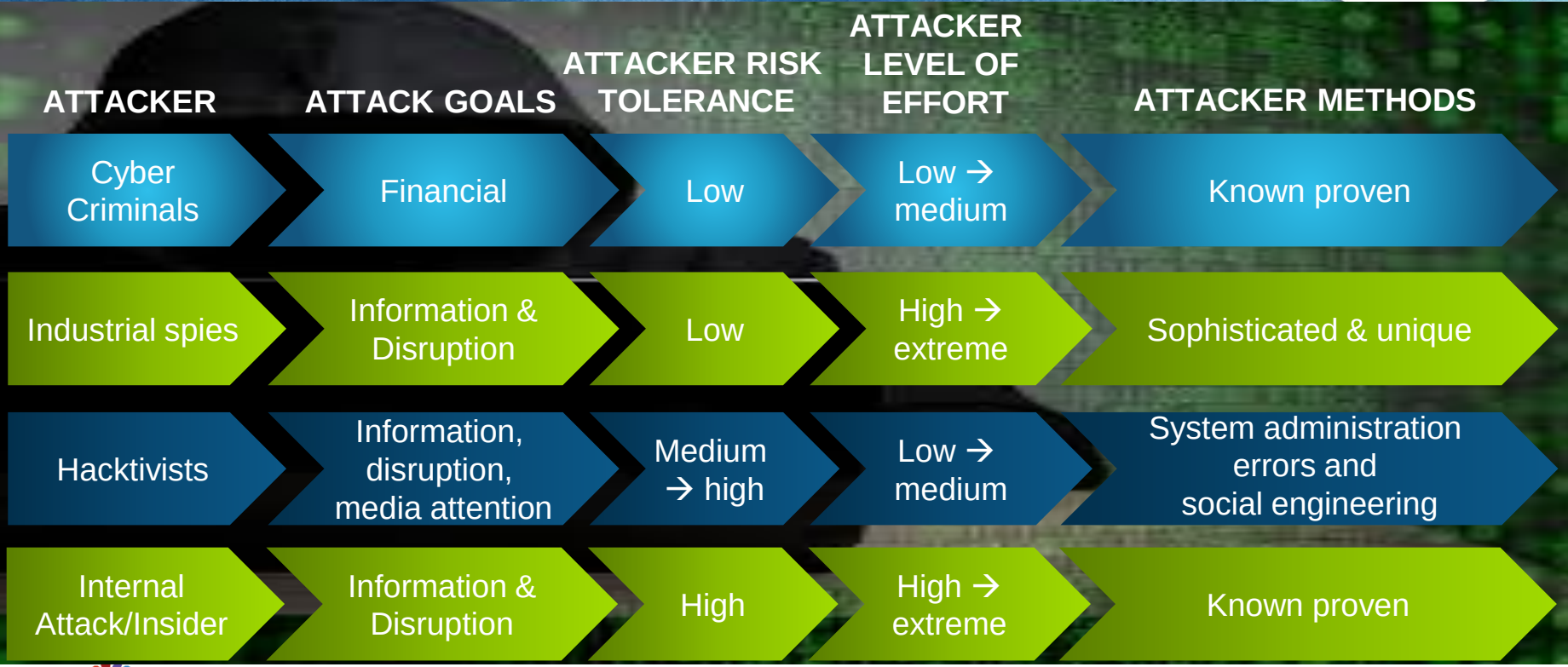
- Reduce security design flaws
- Reduce cost to recover from attacks
- Create effective security requirements
- Know your enemies and their tactics

Security Breaches Can Happen Anywhere

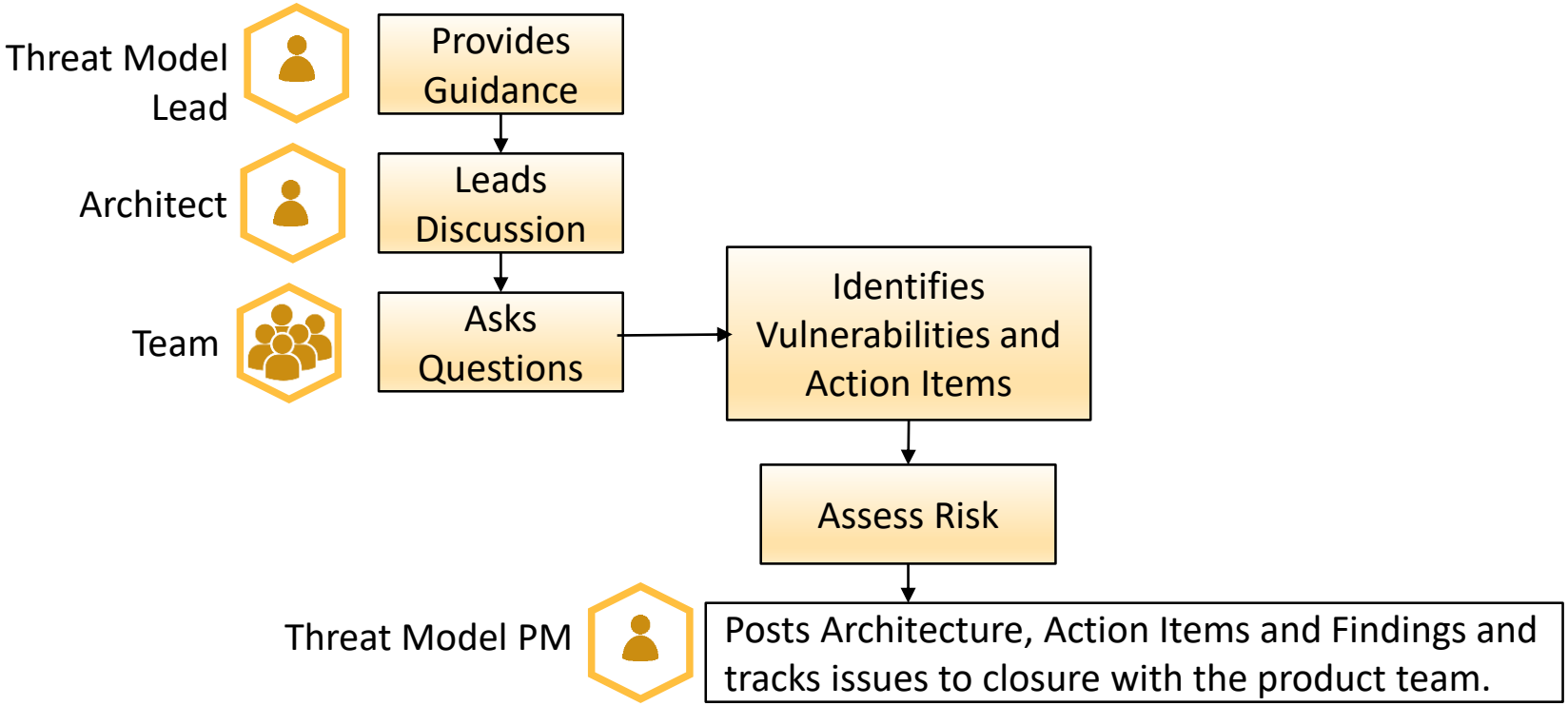
Common Weaknesses and Countermeasures

Weaknesses	Countermeasures
Insufficient API security	API security gateway, OAuth, Tokens, Certificates, Signing Keys
Exposed infrastructure & admin ports	Jump boxes, network ACLs, security groups, iptables, MFA (deprecate telnet!)
Lack of privileged account management & monitoring	Limit shared credentials, local accounts, monitor credential use for abuse. Forward logs to a centralized location, use correlation rules in a SIEM and defined alerts
Hard-coded credentials and API secrets	Key management solutions such as SafeNet, HashiCorp Vault, Ansible Vault, Puppet, Chef Data Bags, SALT, or your company recommended vault
Secure SDLC Practices not integrated into your CI/CD pipeline	Secure the pipeline (e.g. Jenkins, Ansible, Salt, GitHub, other tools), automate static code analysis, use scanning tools web app scanners, Nessus, Qualys)

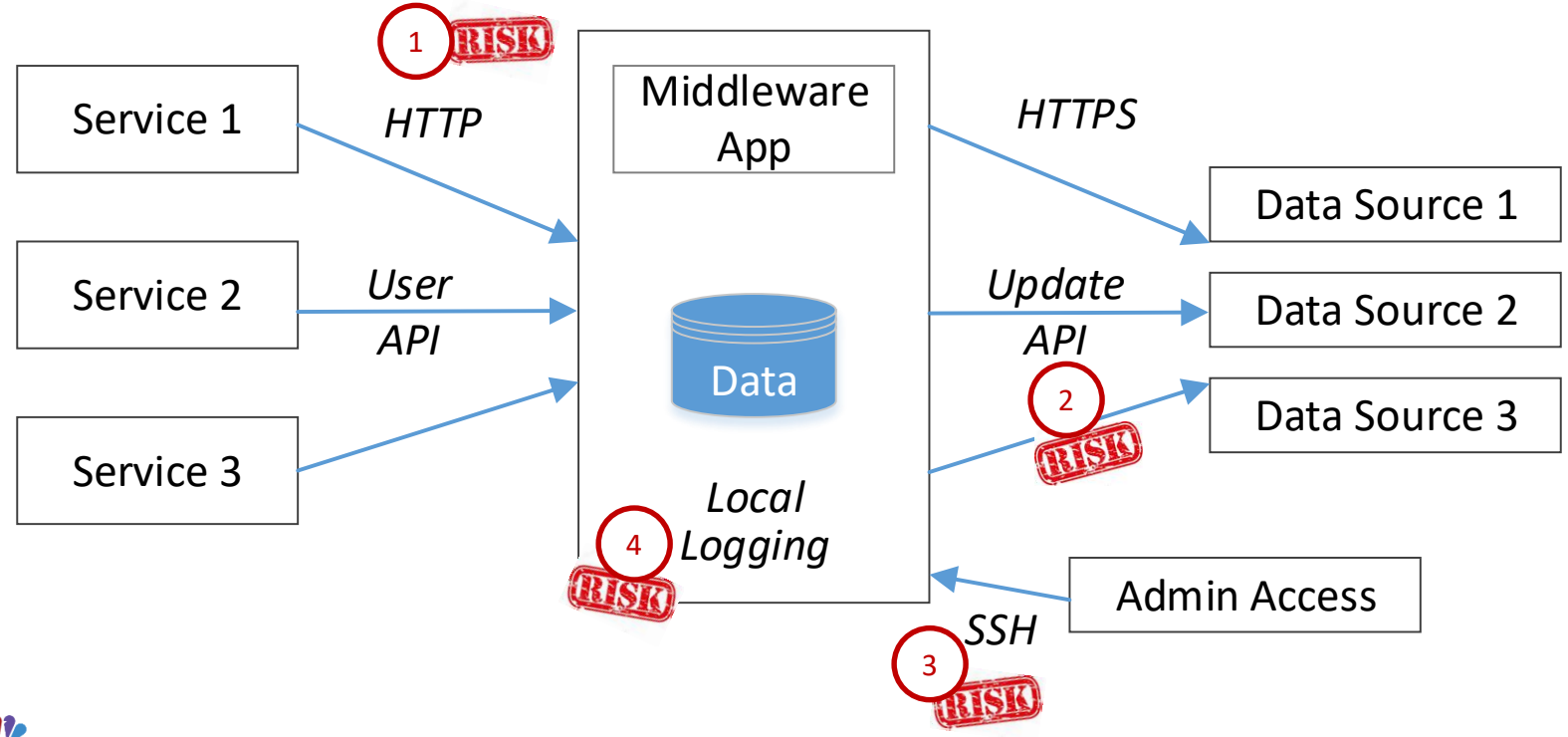
Attacker Profile Exercise



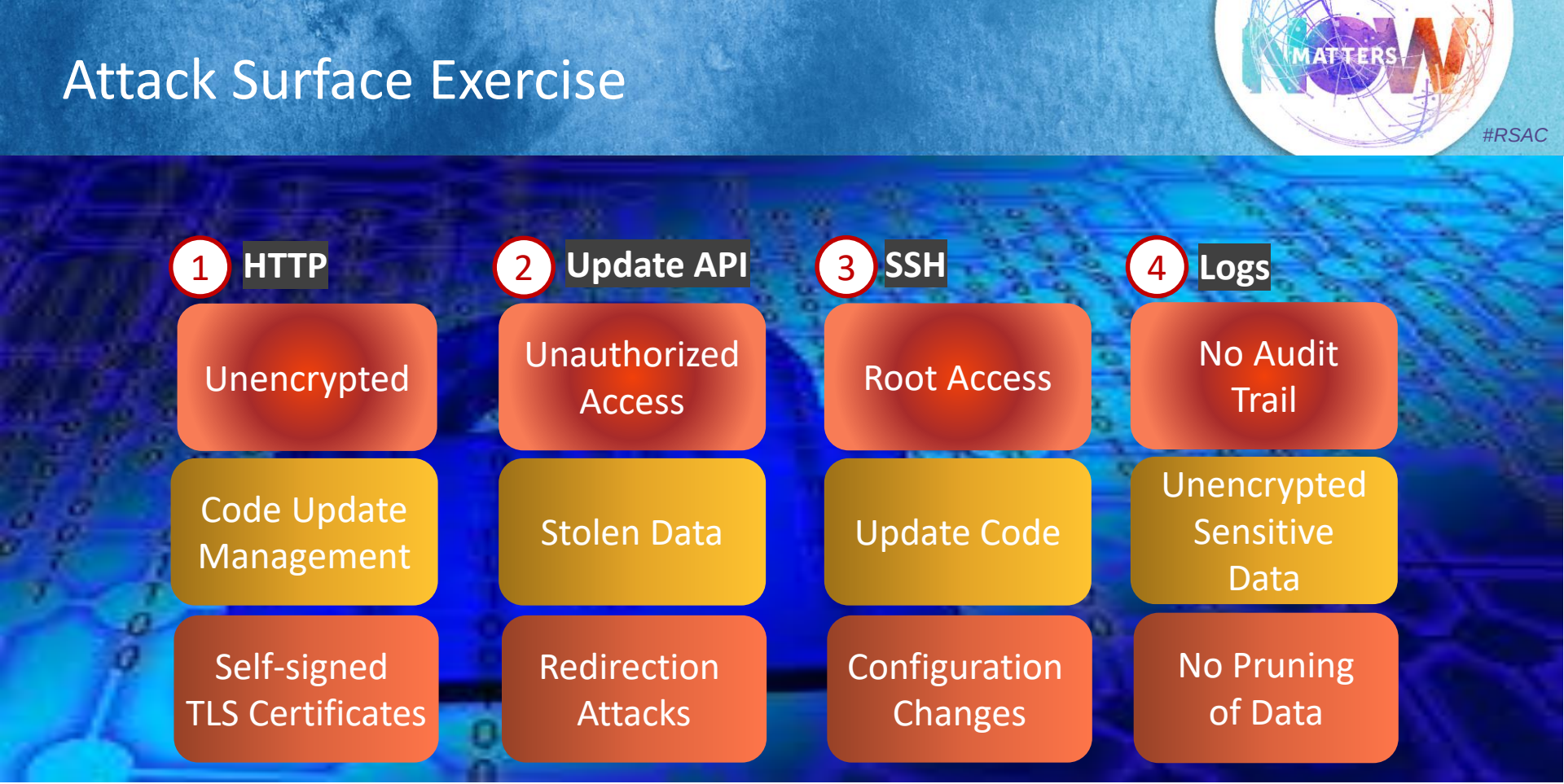
The Process


Threat Model Lead
Provides Guidance
Architect
Leads Discussion
Team
Asks Questions
Identifies Vulnerabilities and Action Items
Assess Risk
Threat Model PM
Posts Architecture, Action Items and Findings and tracks issues to closure with the product team.

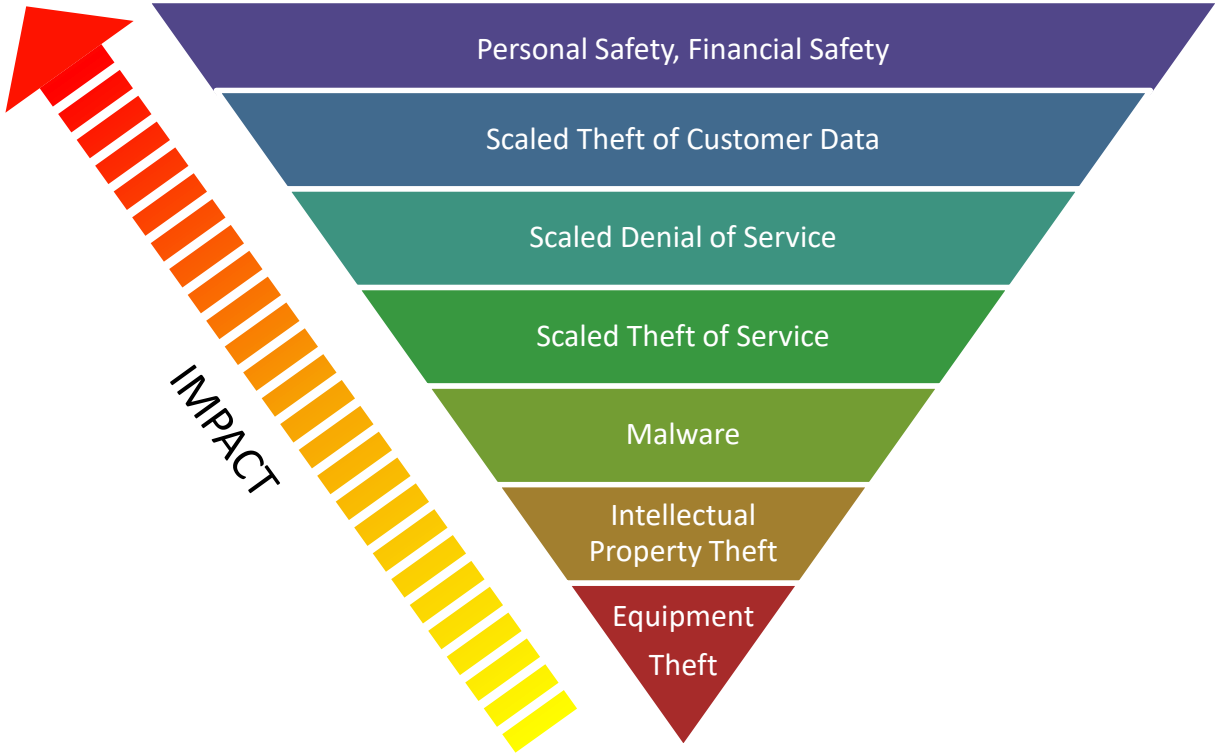
Threat Model Example
Identifying the Attack Surfaces



Attack Surface Exercise



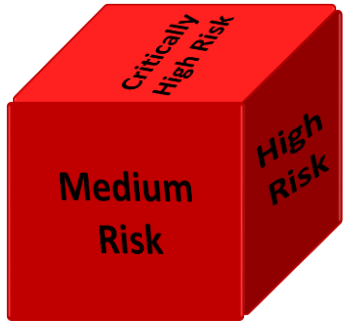
Threat Impacts



Risk

Generalized Risk Equation

Risk = (Threat Impact * Likelihood) / Level of Effort



Summary

- Today you learned about Threats, Impacts and Risk
- How to Perform an Agile and Continuous Threat Model
- Examples of attacks, vulnerabilities and effective countermeasures
- Everyone is responsible for security

Build security in by design, don't bolt it on