DevSecOps Days DC
The Need for Threat Modeling in a DevSecOps World

Simone Curzi, CSSLP

Principal Consultant, Cyber

Microsoft Consulting Services

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Who is Simone Curzi

Principal Consultant

20+ years in Microsoft Services

CSSLP certified

Microsoft WW SDL Community co-Lead

Threat Modeling and Application Security expert

Ongoing collaboration with Companies & Academy

https://simoneonsecurity.com

http://it.linkedin.com/pub/simone-curzi/34/7b3/a35/

https://github.com/simonec73/threatsmanager

Agenda

The DevSecOps Revolution

Is That Enough?

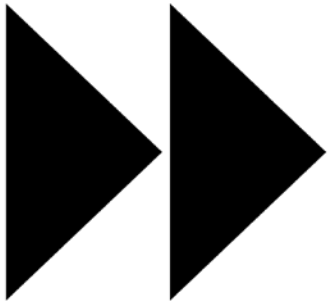
The Answer: Threat Modeling

Conclusions

DEV SEC OPS DAYS

The Need for Threat Modeling in a DevSecOps World

The DevSecOps Revolution



"In the Information Age, one tech year is equivalent to one person's lifetime"

- J.R. Rim

DevOps as the way to accelerate development

DevOps is a set of practices that combines software development (*Dev*) and IT operations (*Ops*). It aims to shorten the systems development life cycle and provide continuous delivery with high software quality.[1][2] DevOps is complementary with Agile software development; several DevOps aspects came from Agile methodology.

Source: https://en.wikipedia.org/wiki/DevOps

Continuous… everything

Continuous Planning

Continuous Collaboration

Continuous Delivery

Continuous Learning

Continuous Security

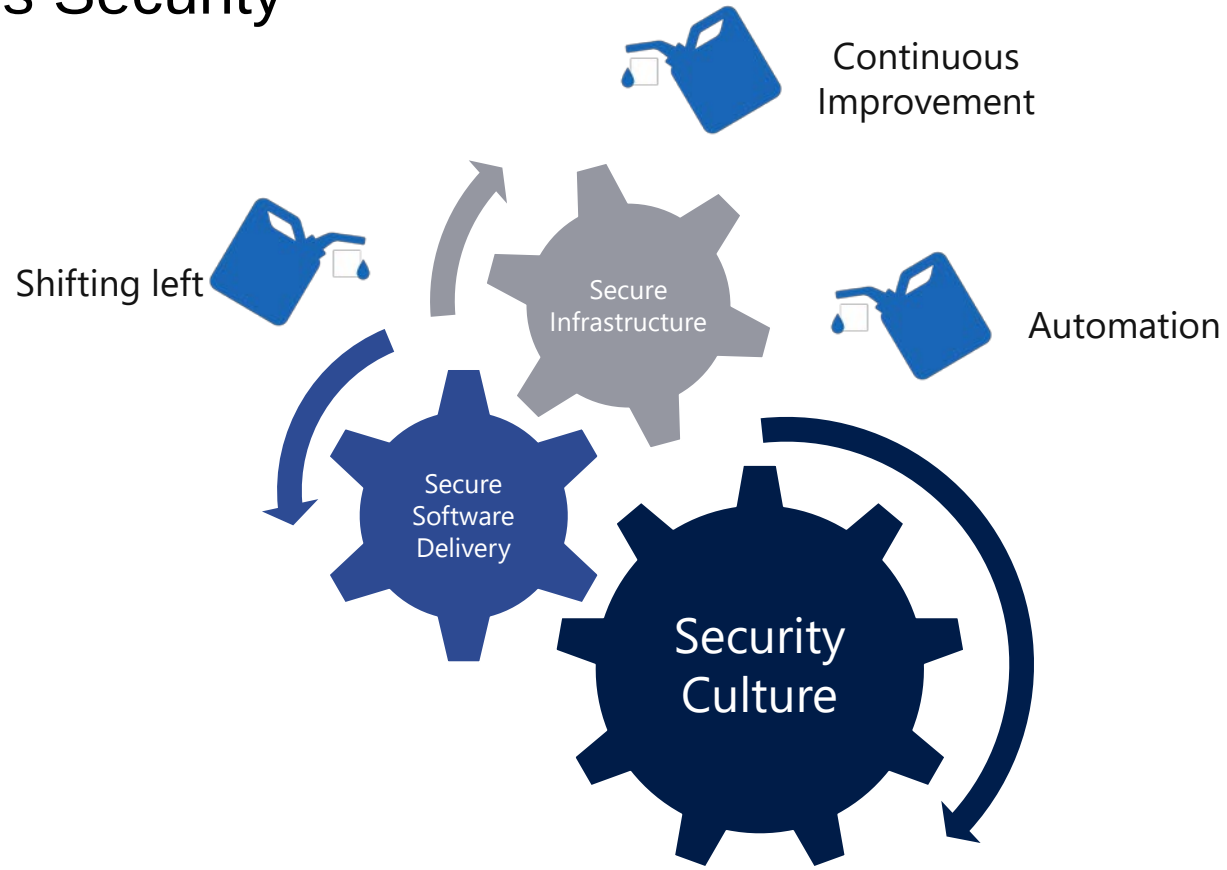
Continuous Quality

Continuous Integration

Continuous Improvements

Continuous Operations

Continuous Security



Continuous Security Automation

Static Application Security Testing (SAST)

Dynamic Application Security Testing (DAST)

Software Composition Analysis (SCA)

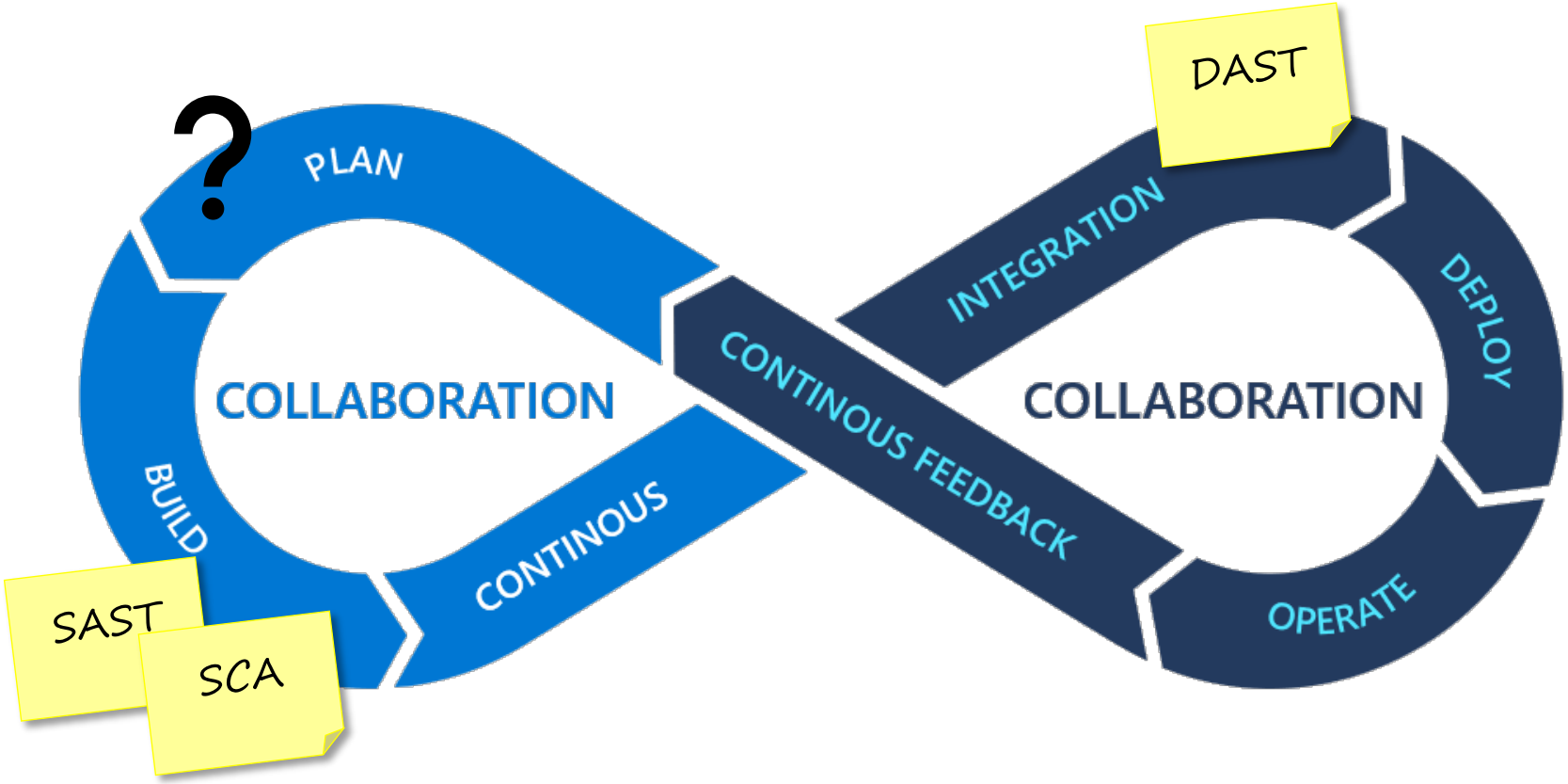
DEV SEC OPS DAYS

The Need for Threat Modeling in a DevSecOps World

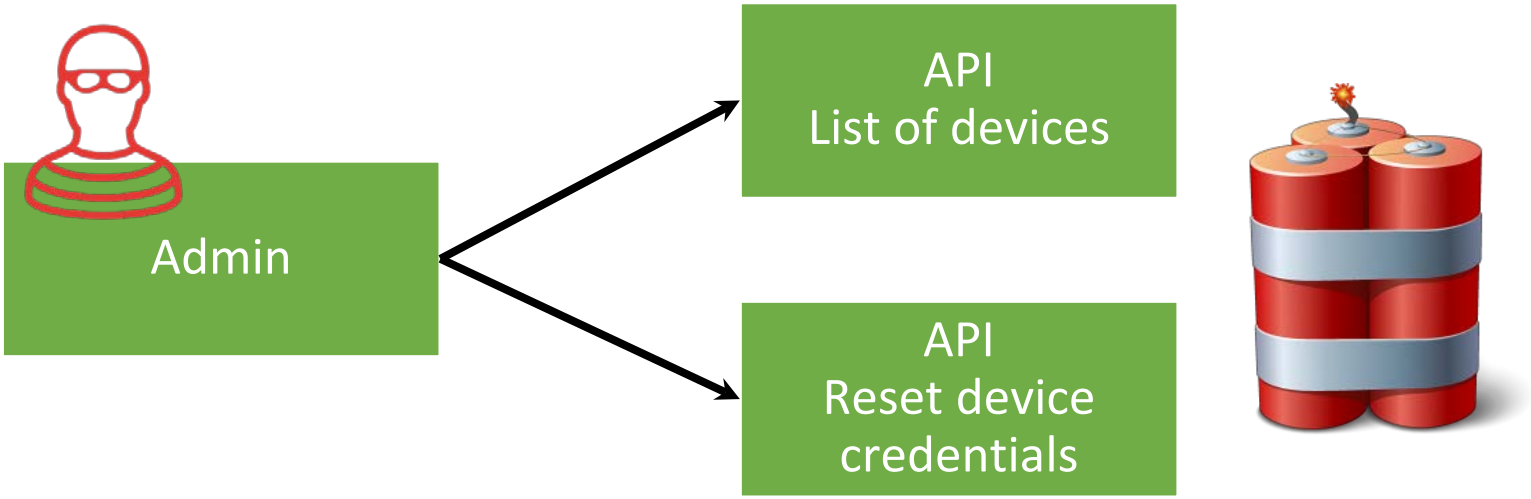
Is That Enough?

The One Million Dollar Question!

Placing the Automation Tools



A Real Life Example



Cost of 1h of disservice per device: 40K USD
Fleet of 1000 devices
Duration of an incident: Avg 2 hrs

80M USD

Automation doesn’t know your Business

So, is the current approach enough?

Tools, Best Practices, Checklists
Policies, Penetration Tests

EXPOSURE
IS IT ON INTERNET?

SENSITIVITY
BUSINESS CRITICAL?

REGULATIONS
INCLUDING PRIVACY

COST
IS IT TOO IMPORTANT?

DEV SEC OPS DAYS

The Need for Threat Modeling in a DevSecOps World

The Answer: Threat Modeling

Threat Modeling

Threat Modeling is a process to understand **security threats** to a system, determine **risks** from those threats, and establish appropriate **mitigations**.

The Threat Modeling Process (simplified)

DEV SEC OPS DAYS

01

Understand

- The Diagram

02

Analyze

- The Threats

03

Solve

- The Mitigations

What should you Threat Model?

The solution

CI/CD

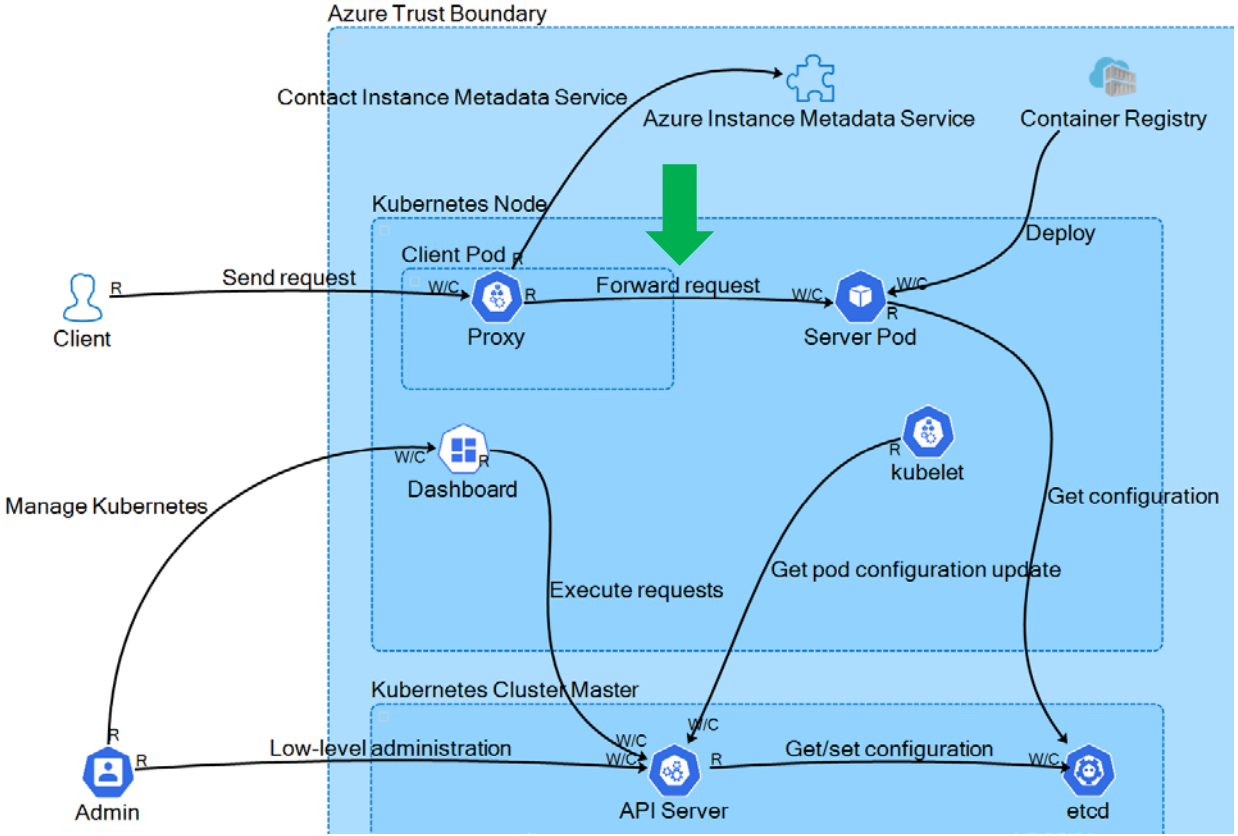
Administration

DevSecOps environment

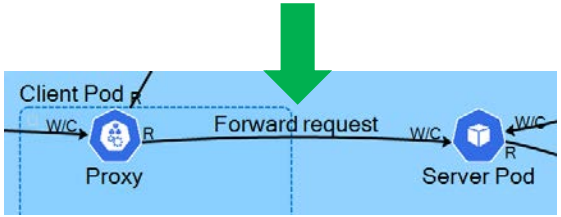
Specific Scenarios

(ex.: Data Scientist)

“I do Threat Modeling! I use tool XYZ!”



How many Threat Modeling products identify Threats



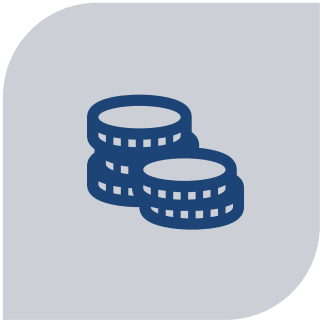
Would you be able to understand anything from that???

DEV SEC OPS DAYS

The Need for Threat Modeling in a DevSecOps World

Conclusions

The advantages of adopting Threat Modeling in DevSecOps



Starting Security early, lowers costs

Catches Design issues

Helps to evaluate new risk factors early

YOU can be the best Threat Modeling Tool!

Knowledge about potential attacks

Holistic approach

Skeptic, never assuming mindset

Existing Threat Modeling Tools have an important role to play

Most threats are common

Many of them can learn something about your Business

Some are Integrated with Tracking Tools and Boards

DEV SEC OPS DAYS

The Need for Threat Modeling in a DevSecOps World

THANK YOU!