strike

Threat Modeling 101

Marco Bicca
Senior Security PM
Core Devices and Gaming Security Services Assurance (CDG SSA)

Threat Modeling 101. Am I in the right spot?

- If you have already done Threat Models this might not be for you. Go check it out for other tracks while you still can ☺
- This is an introductory presentation about Threat Modeling.

Content and links

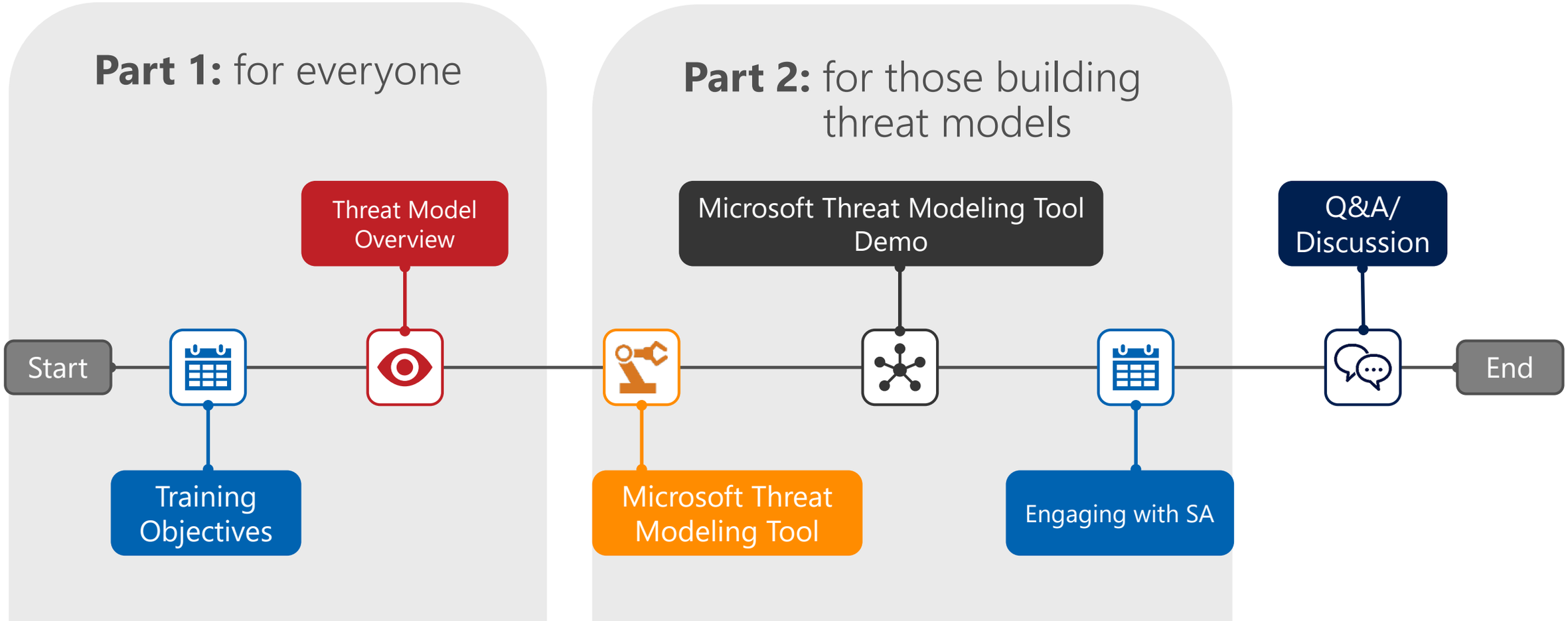
- Sessions will be recorded and available online at https://strike next week.

A real analogy ….

Do you play an instrument?
Do you do any sports?

Purpose of this training:

Develop a critical muscle that will enable us to deliver trusted content to our customers.



Training objectives

Understand the **security mindset**.

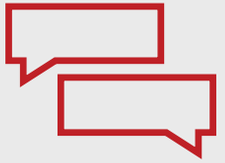
Understand threat modeling and **how to prepare for and participate in a security review**.

Understand that **security *is* part of your job**.

Enabled to **take action**.

Understand **how to build a threat model**.

Start the **conversation**.



Part 1: threat model overview

Dataflow Diagram (DFD) + model analysis

Threat Model

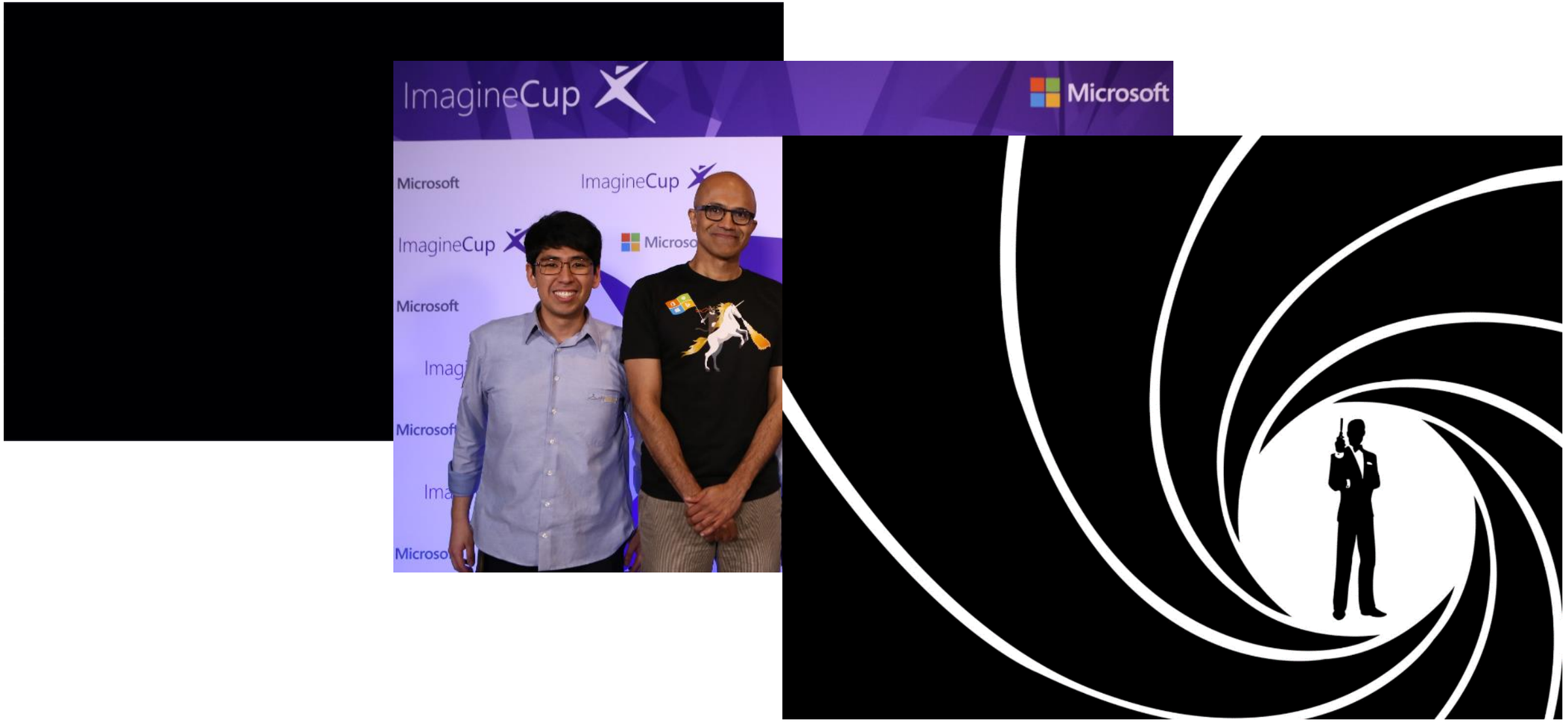
=

Dataflow Diagram (DFD)

+

Model Analysis

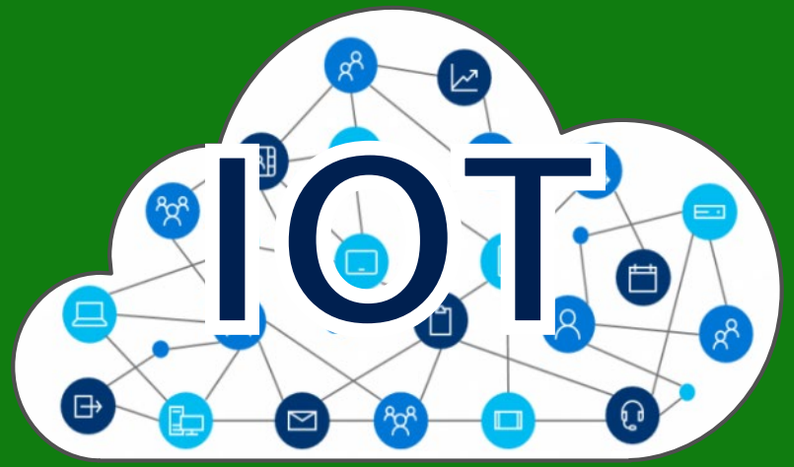
Why model my service?



How to diagram in the security mindset

- **You own security.**
- **Understanding your environment is critical.**
- To get started, ask yourself, “what keeps you up at night?”
- In other words, “how would you attack your own service?”

When to model?



Threat model maintenance

- Reorg
- New component
- New feature
- New tool
- Major changes to the service
- Deprecation of the service

Threat Model

=

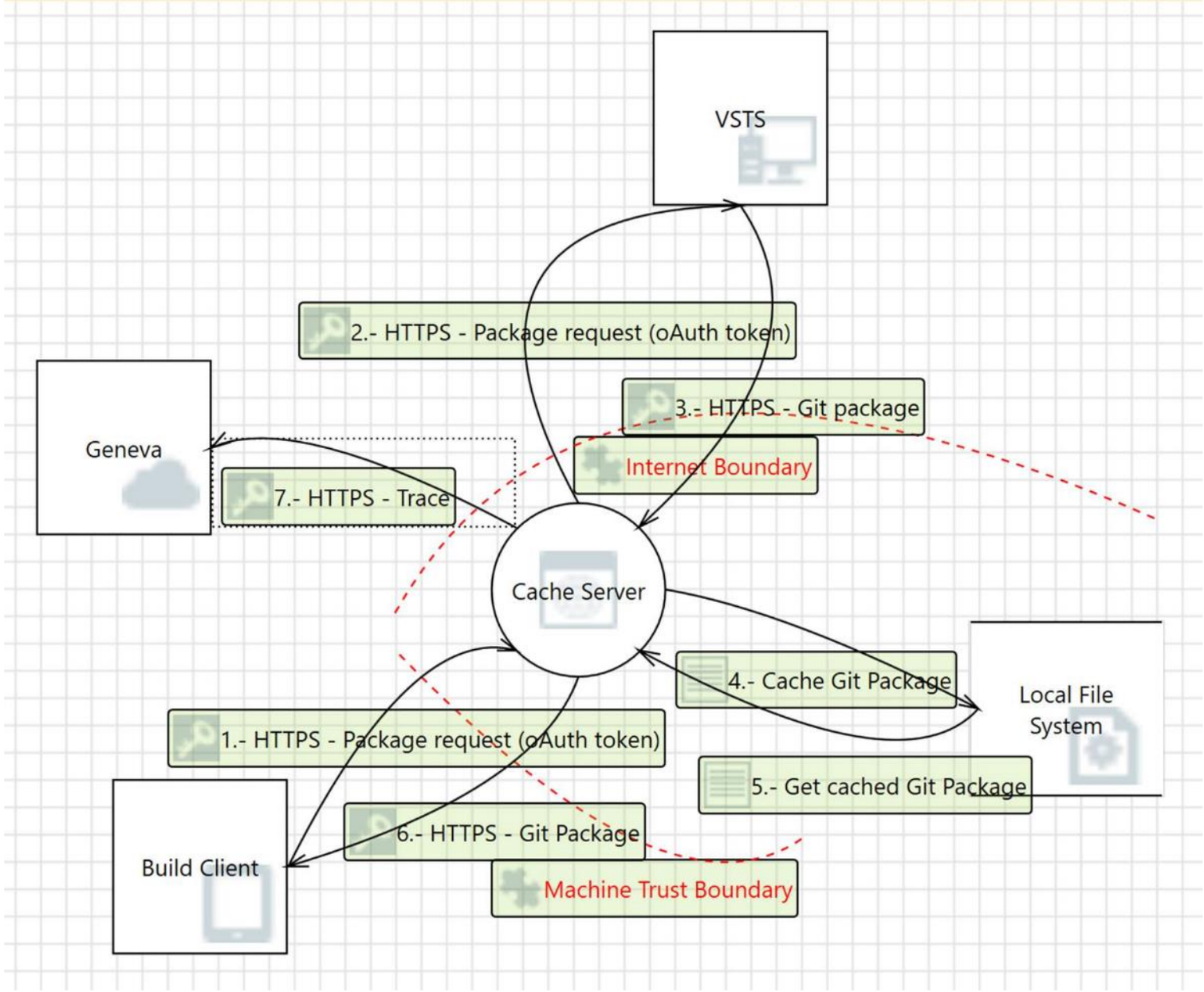
Dataflow Diagram (DFD)

+

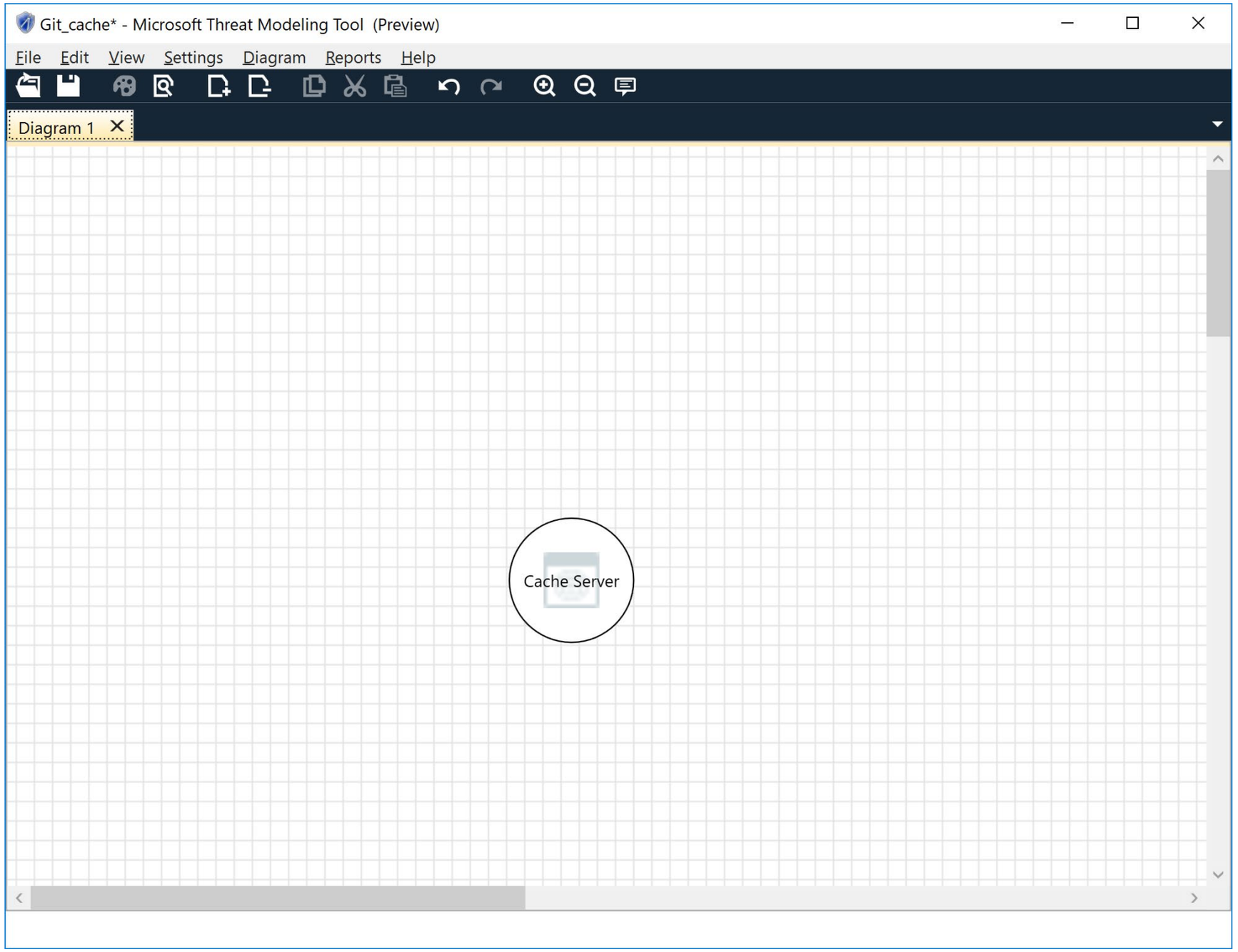
Model Analysis

Dataflow diagram example:

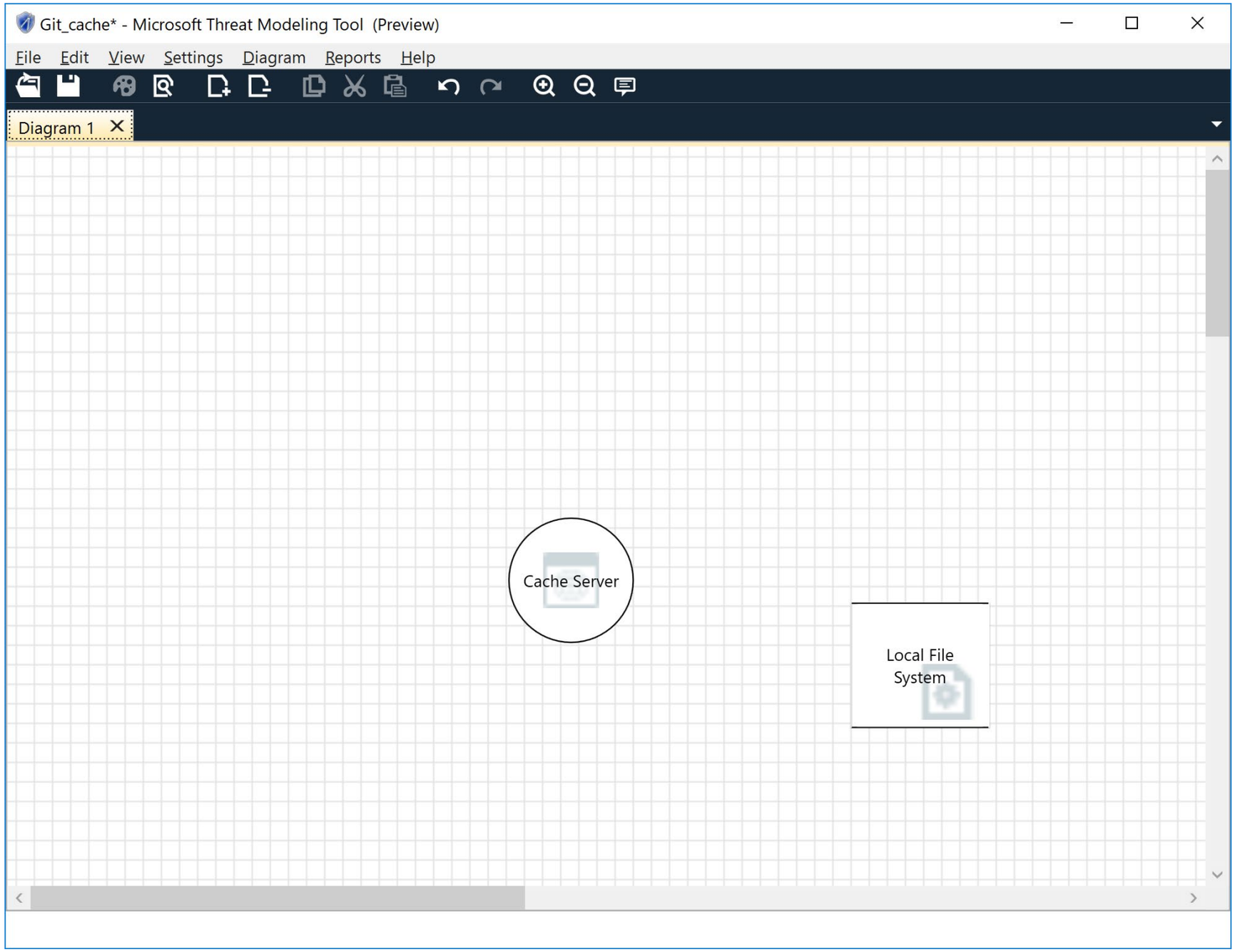
GIT cache server



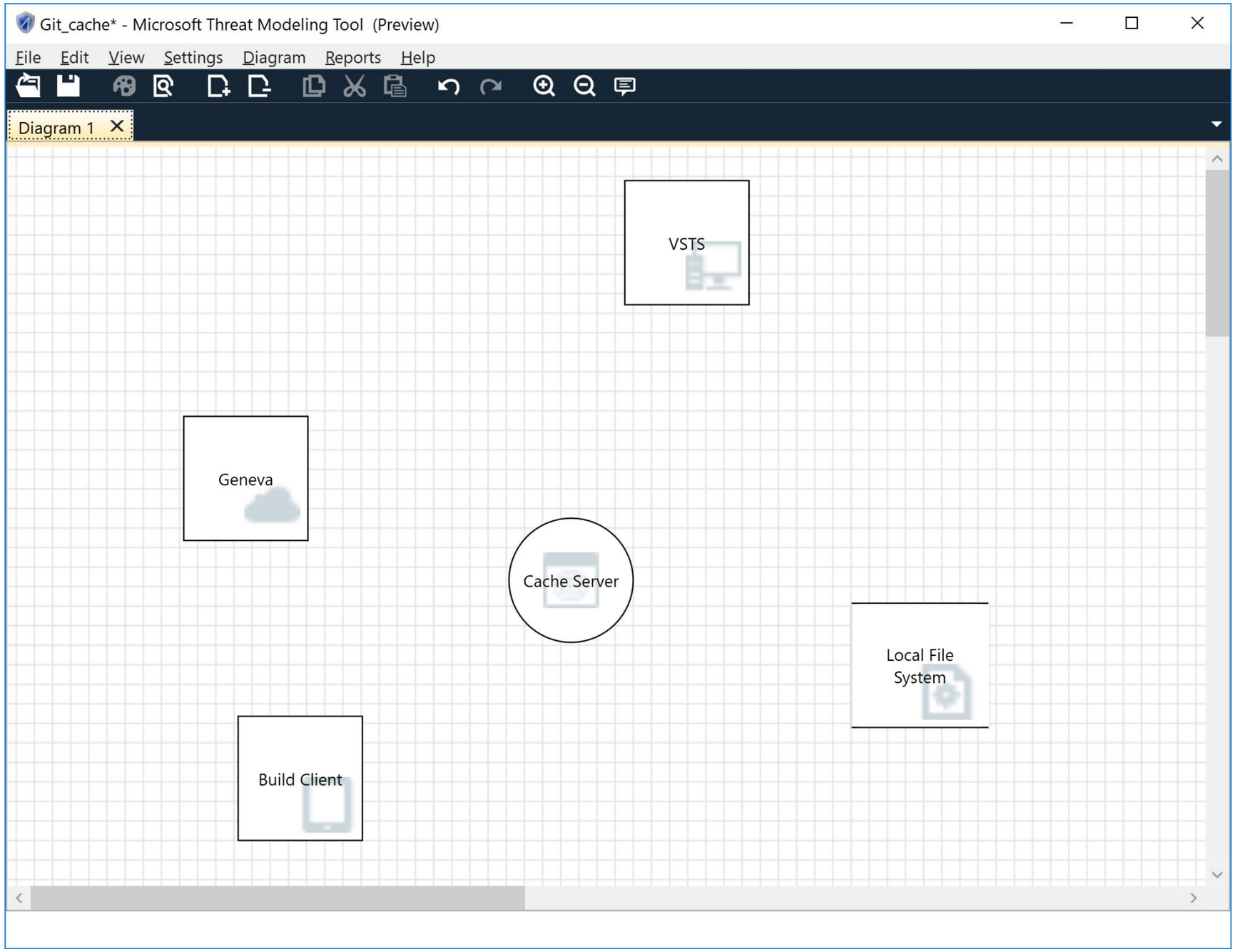
Start with your Process(es).



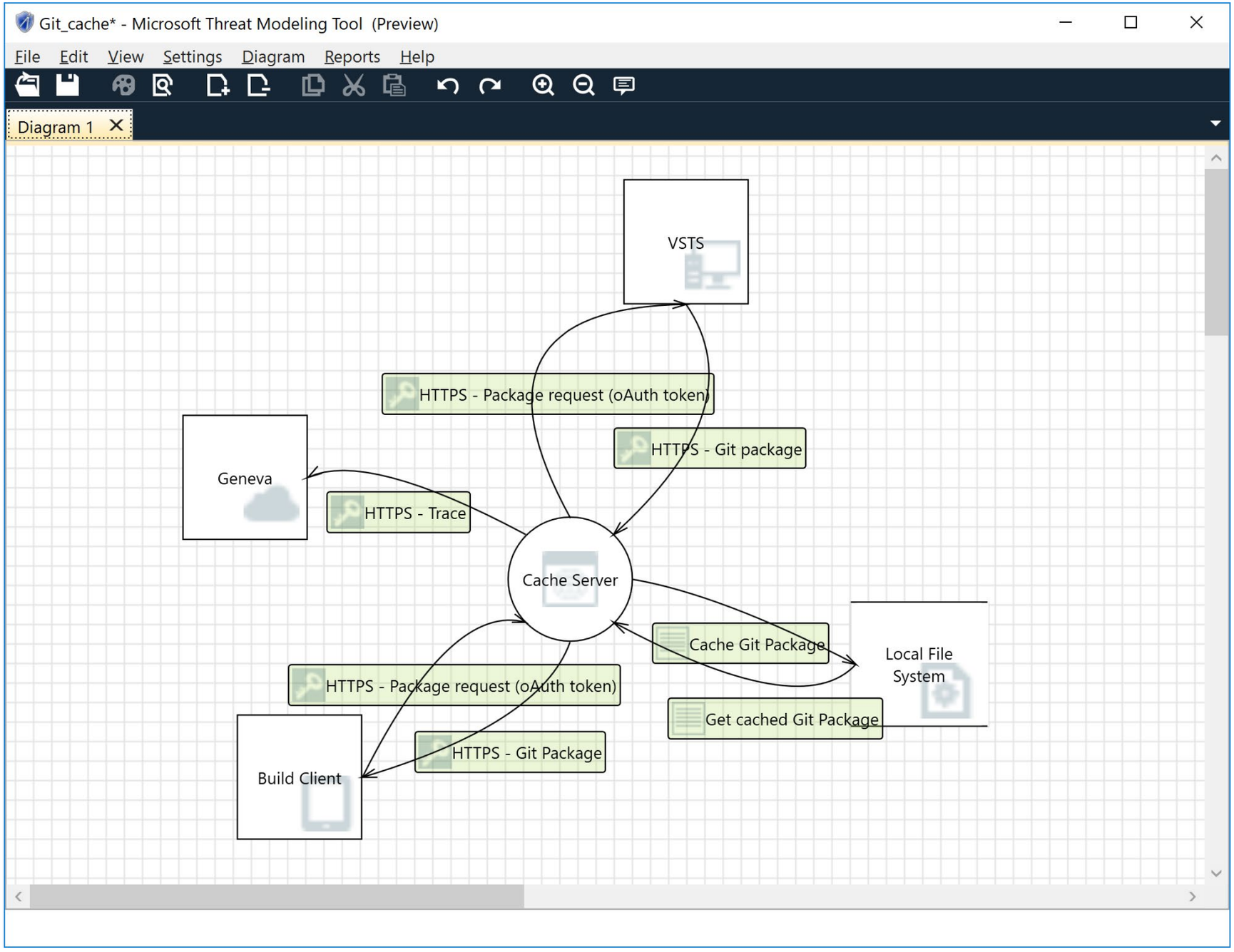
Add its Storage.



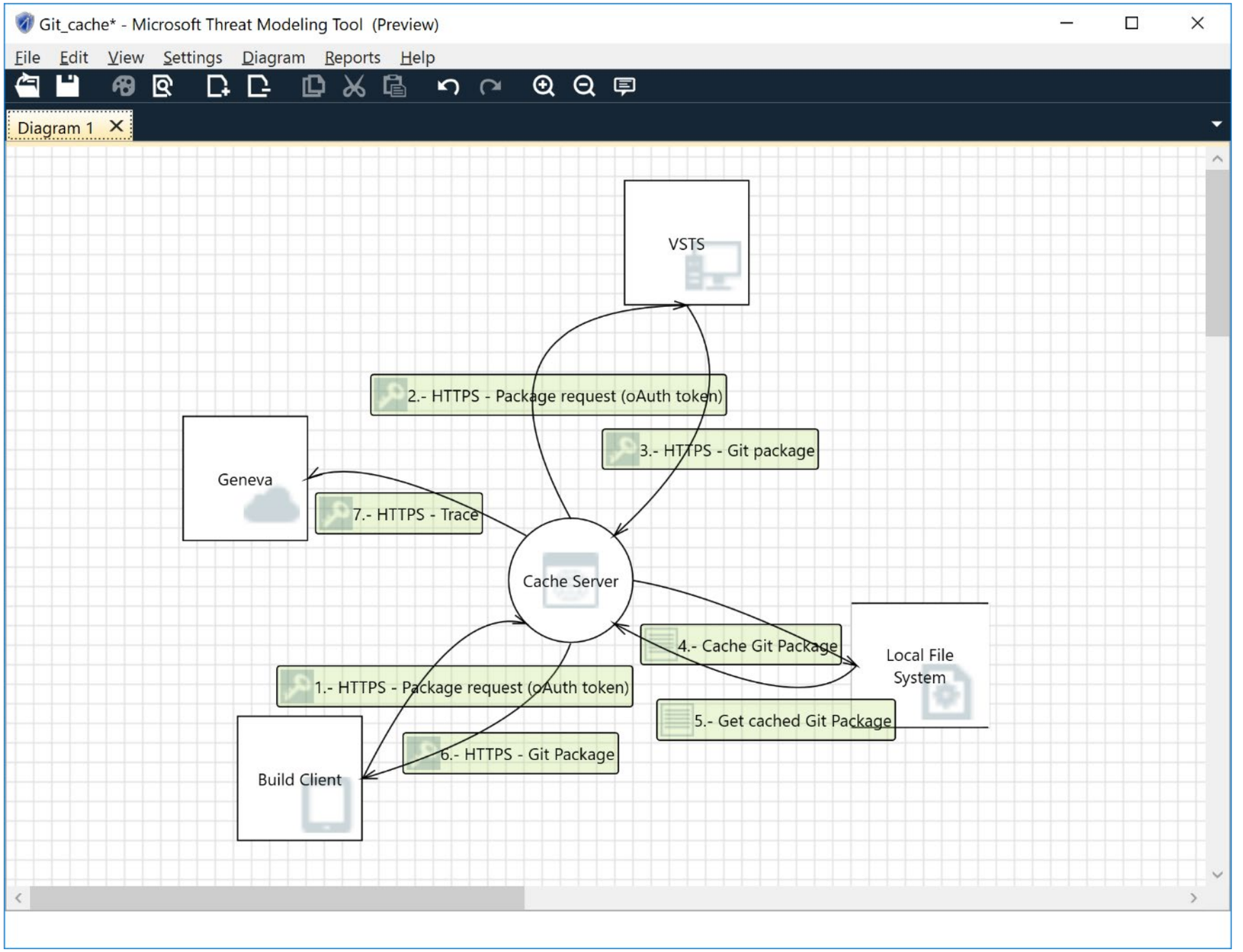
Add external interactors.



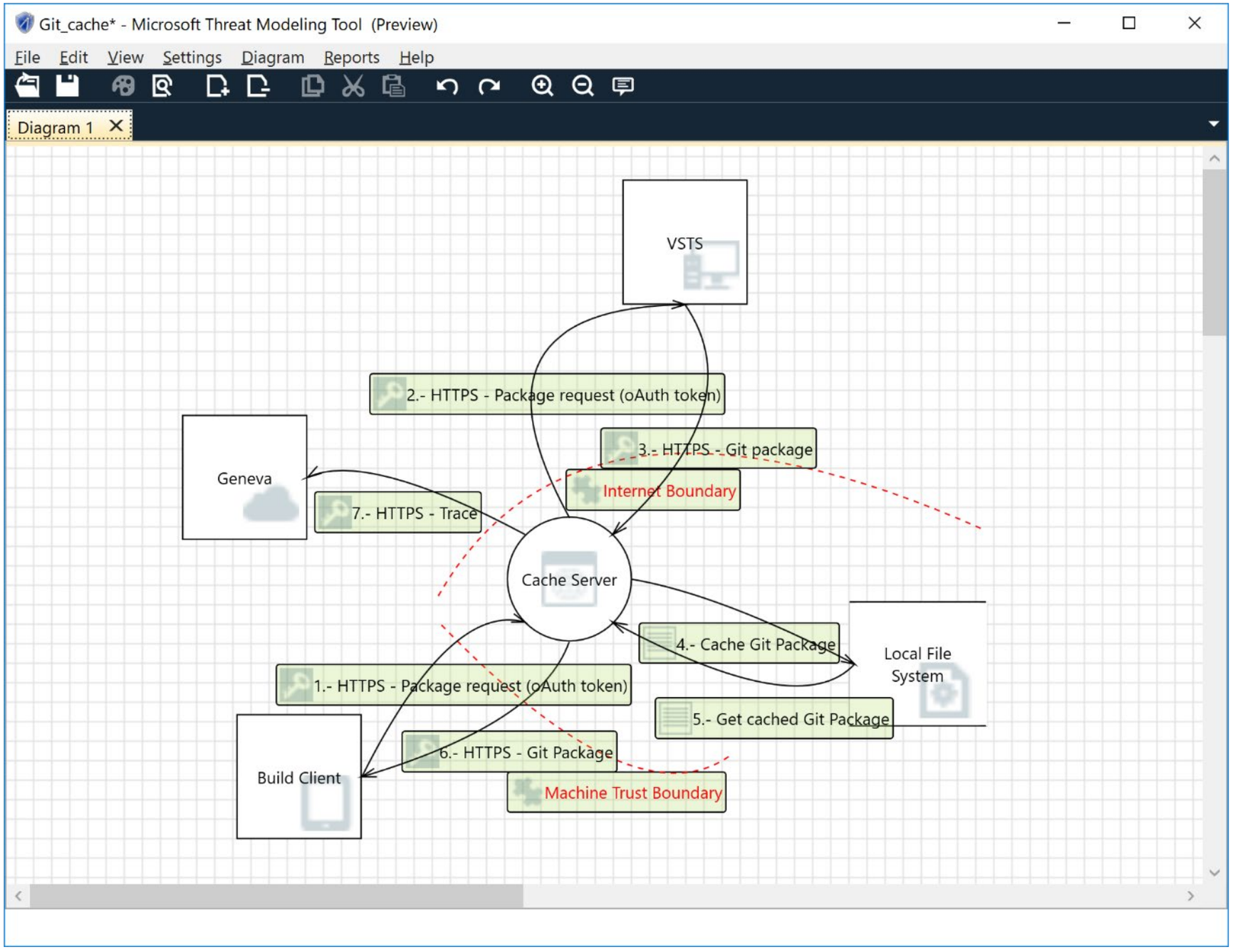
Add Dataflows.



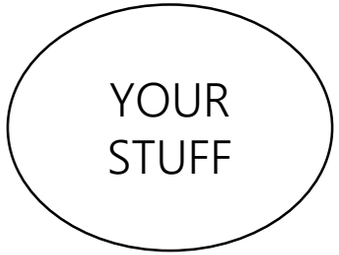
Add numbering.



Add Trust Boundaries.



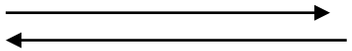
Dataflow diagram elements



Circles: your service and processes
(i.e. your code or under your control)

Squares: external interactors (users, 3rd party services
and other Microsoft services not under your control)

Lines: data storage
(databases, Azure storage, shared files)

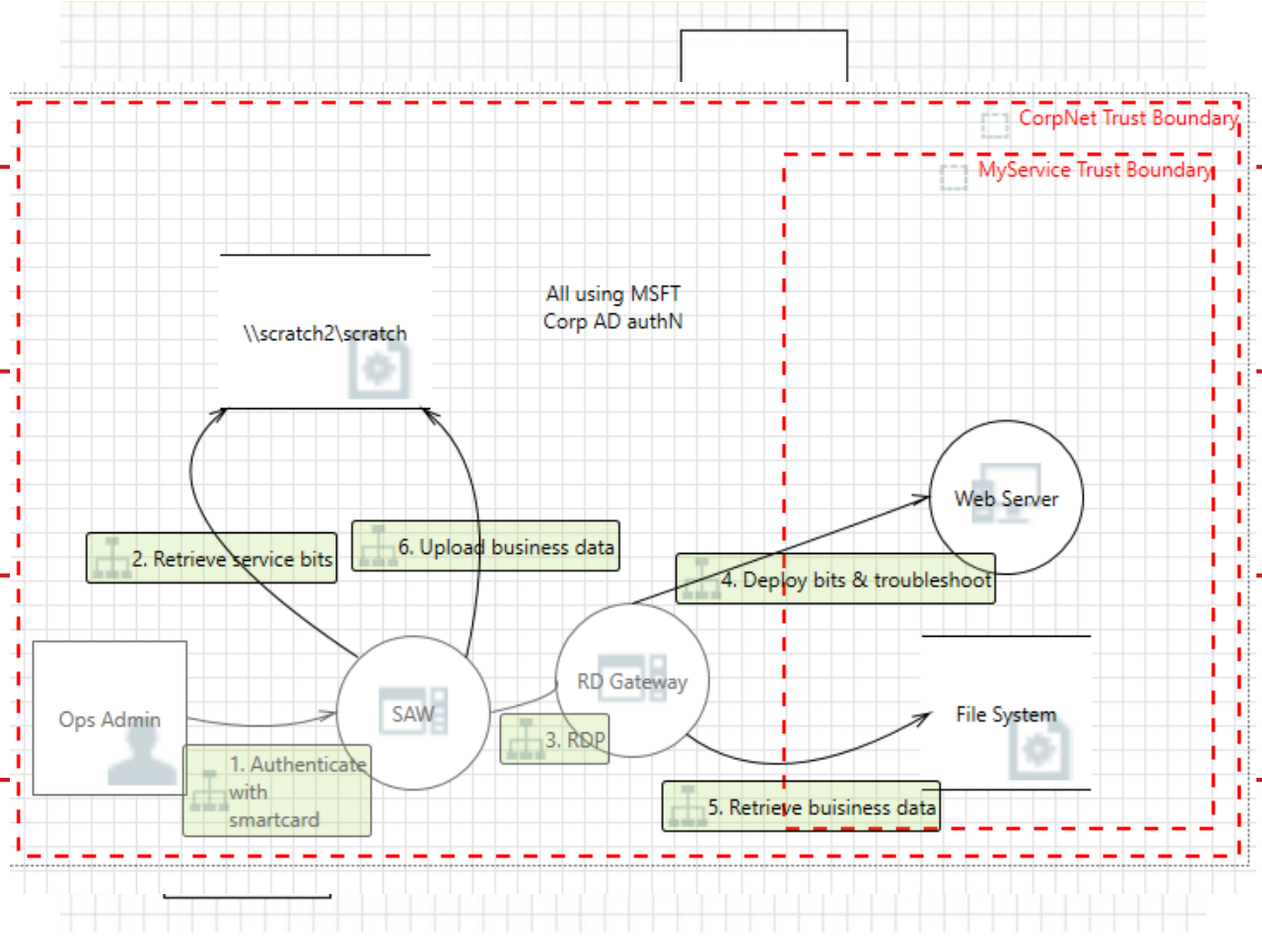


Arrows: data, control, and influence move between elements

Dashed Lines: privilege boundary

Dataflow diagram complete

- Dependencies
- Machine roles and services
- Storage entities
- Relevant interactions



Threat Model

=

Dataflow Diagram

+

Model Analysis

Model analysis

STRIDE represents these threat categories:

Spoofing (of user identity)
Tampering
Repudiation
Information Disclosure (privacy breach or data leak)
Denial of Service (DoS)
Elevation of Privilege

Spoofing

Framing questions:

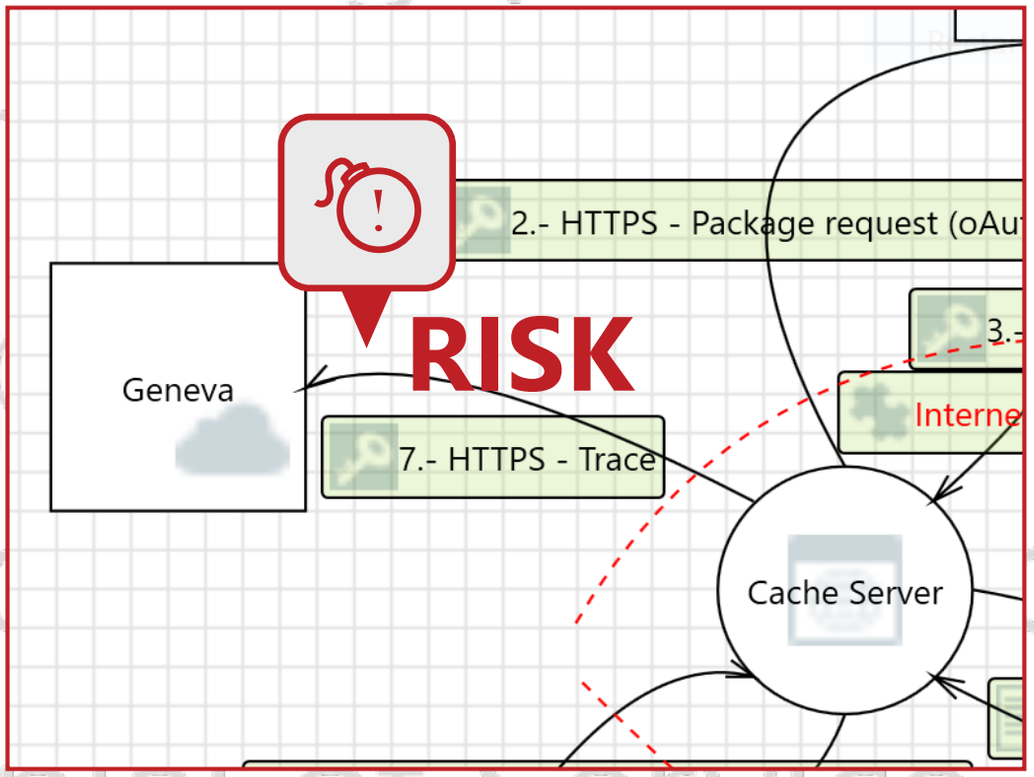
- How do we know the human user is who they claim to be?
- How do users know we are who we claim to be?
- How do you identify entities in a service to service communication?

Spoofing (of user iden
Tam
Rep
Info osur
Denial of Service (Do
Elevation of Privilege

Spoofing

Someone could try to spoof Geneva to the Cache Server.

How can the Cache Server know Geneva is really Geneva?



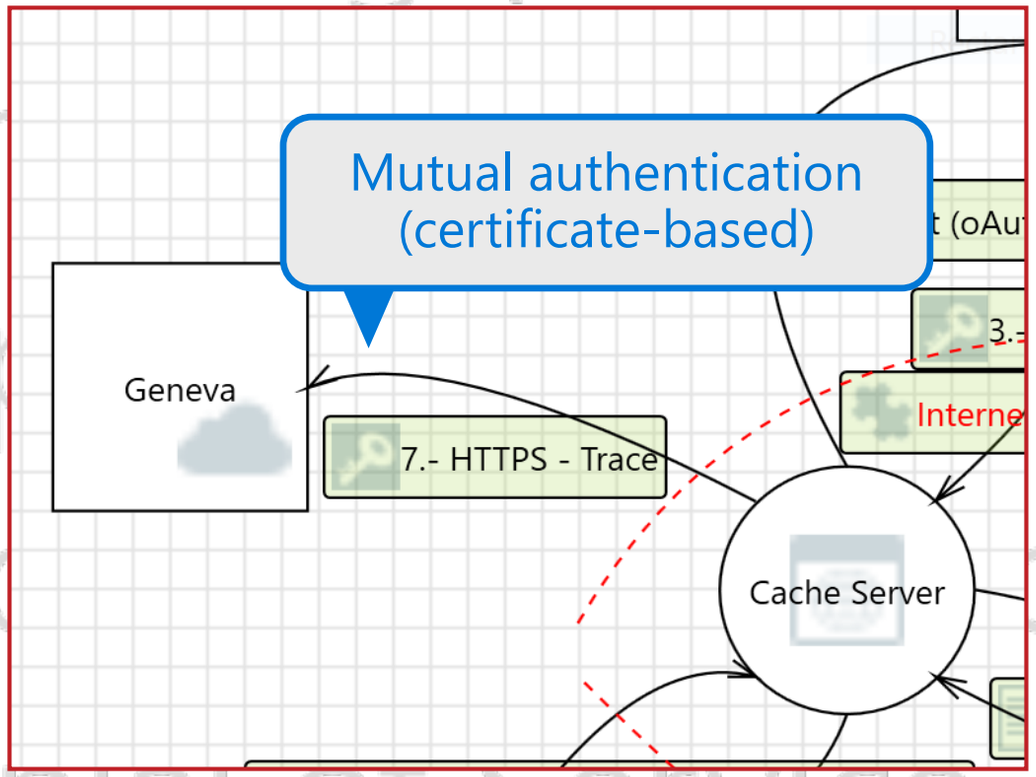
Spoofing

How do we mitigate?

Authentication

Mutual Authentication (certificate based)

- Consider Certificate pinning



Tampering

Framing questions:

- Can somebody modify the data in transit?
- Can an unauthorized user modify the data at rest?
- Who can modify the binaries we deploy?

Spoofing (of user iden

T

R

I

D

E

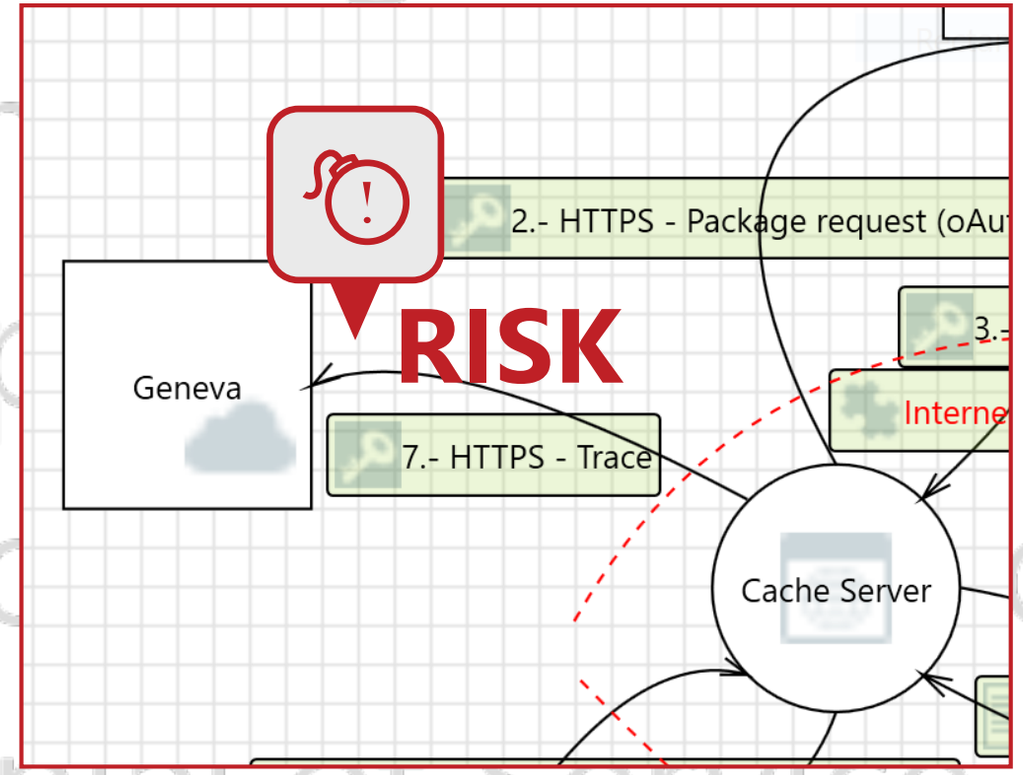
Denial of Service (Do

Elevation of Privilege

Tampering

Someone might tamper with the logs before they arrive at Geneva.

How can we prevent or detect that?



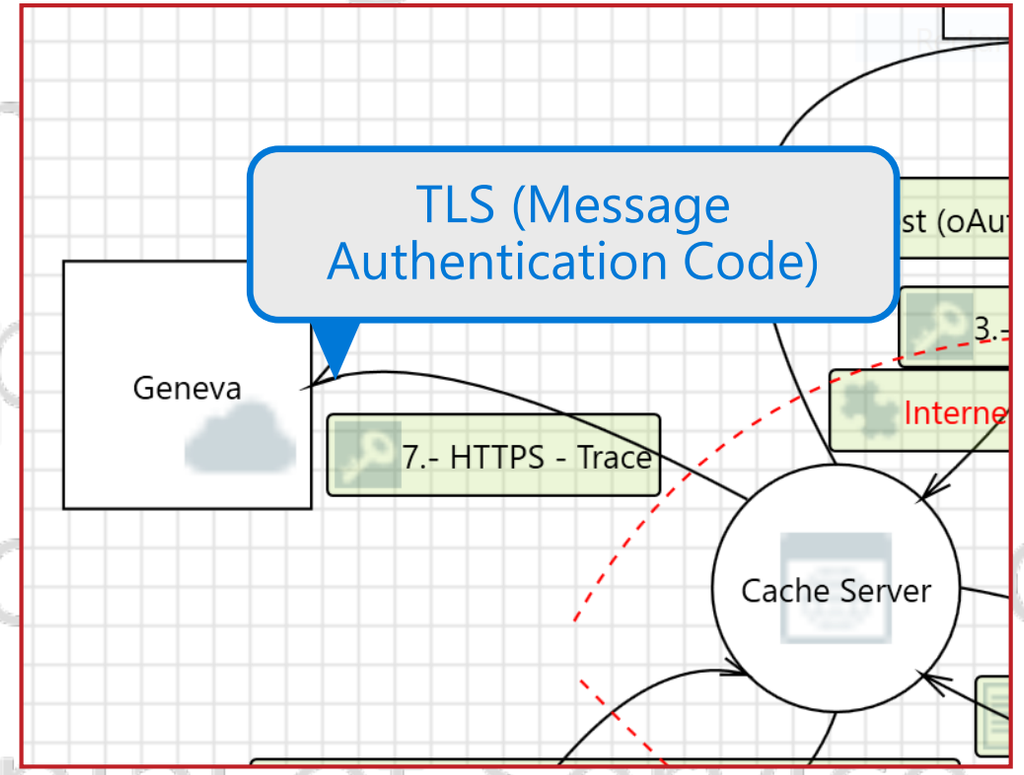
Spoofing (of user ide
Tar
Rep
Info
osur
Denial of Service (Do
Elevation of Privilege

Tampering

How do we mitigate?

- Using protocols that provide integrity protection (i.e. HTTPS).
- For data-at-rest, use digital signatures or Authenticated Encryption (AE).
- Digital signature on executables.

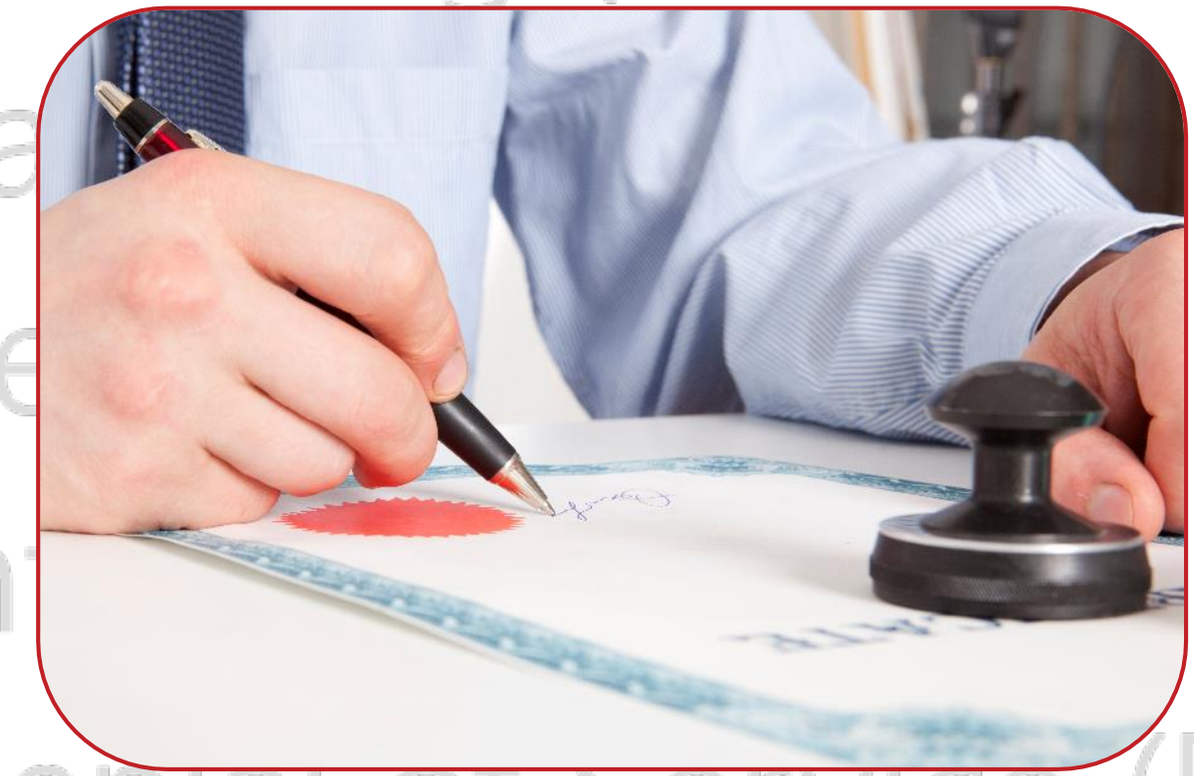
*Transport Layer Security (TLS)



Repudiation

Framing question:

Can the user claim they did not commit an action on the server?



Spoofing (of user ide

T a

R e

I n sur

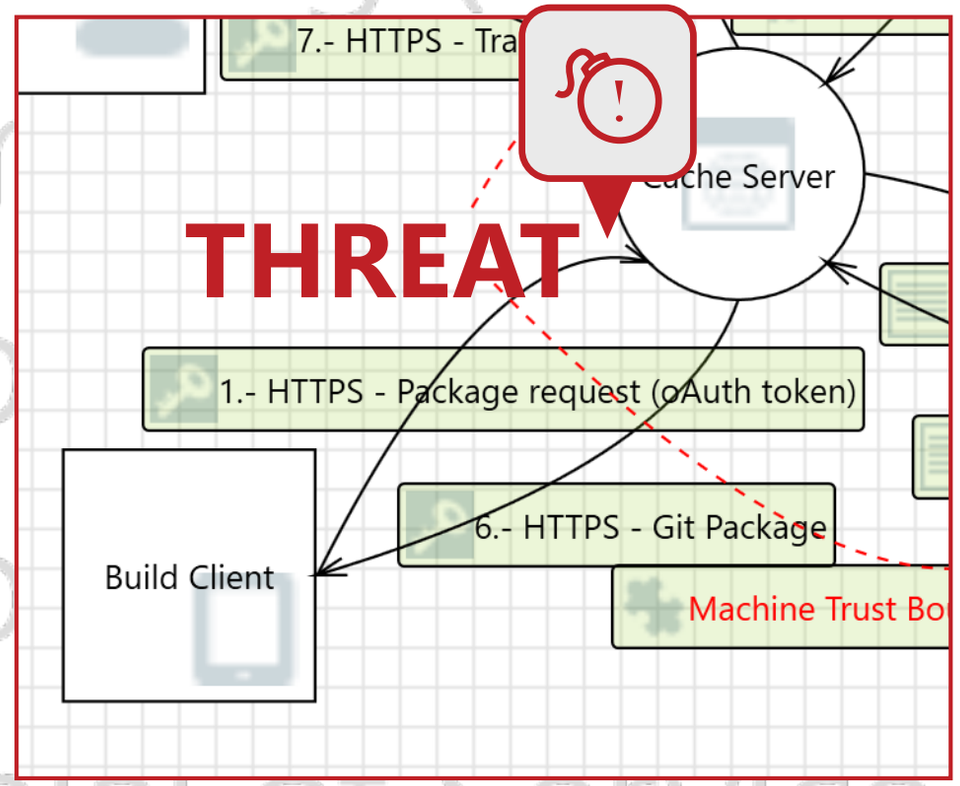
D enial of Service (Do

E levation of Privilege

Repudiation

Build Client could repudiate receipt of the package it requested.

How can Cache Server prove that it sent the right package?

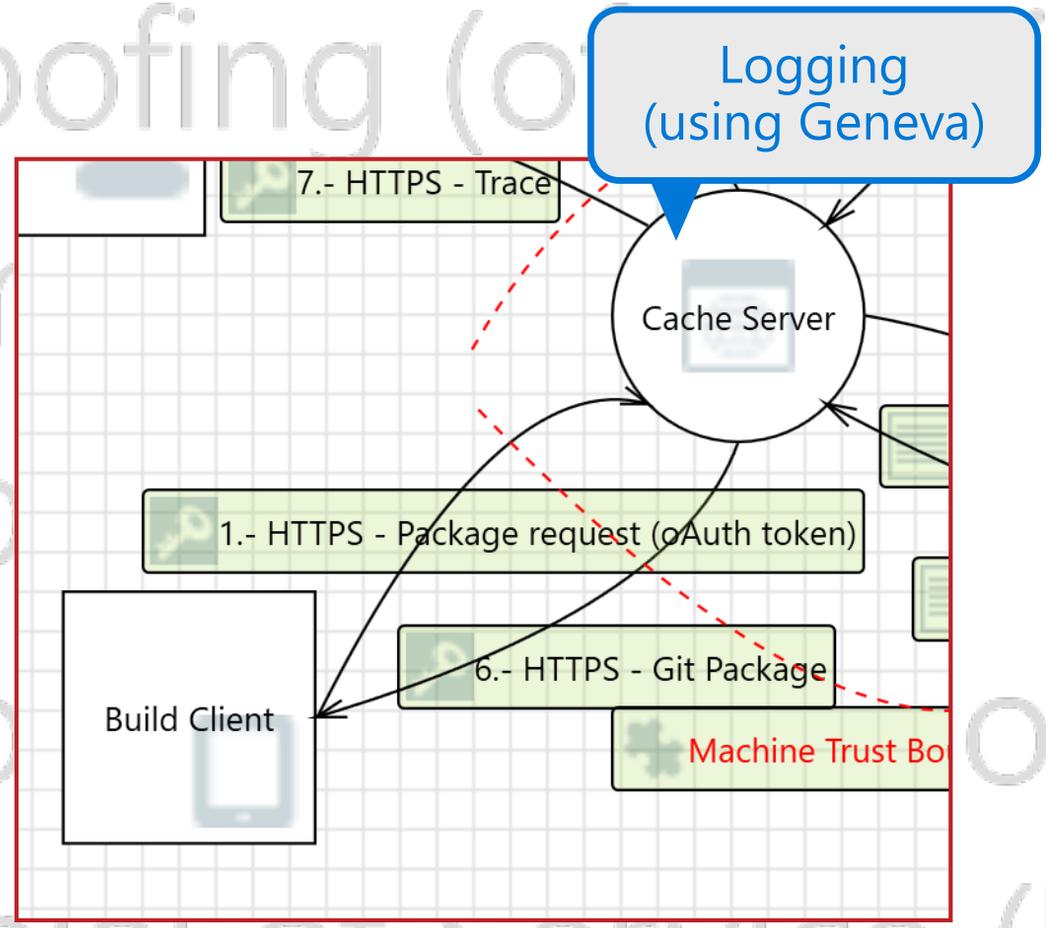


Spoofing (of user ide
Tam
Rep
Info
osur
Denial of Service (Do
Elevation of Privilege

Repudiation

How do we mitigate?

- Application logging
- Audit logs
- Event logs
- Monitoring

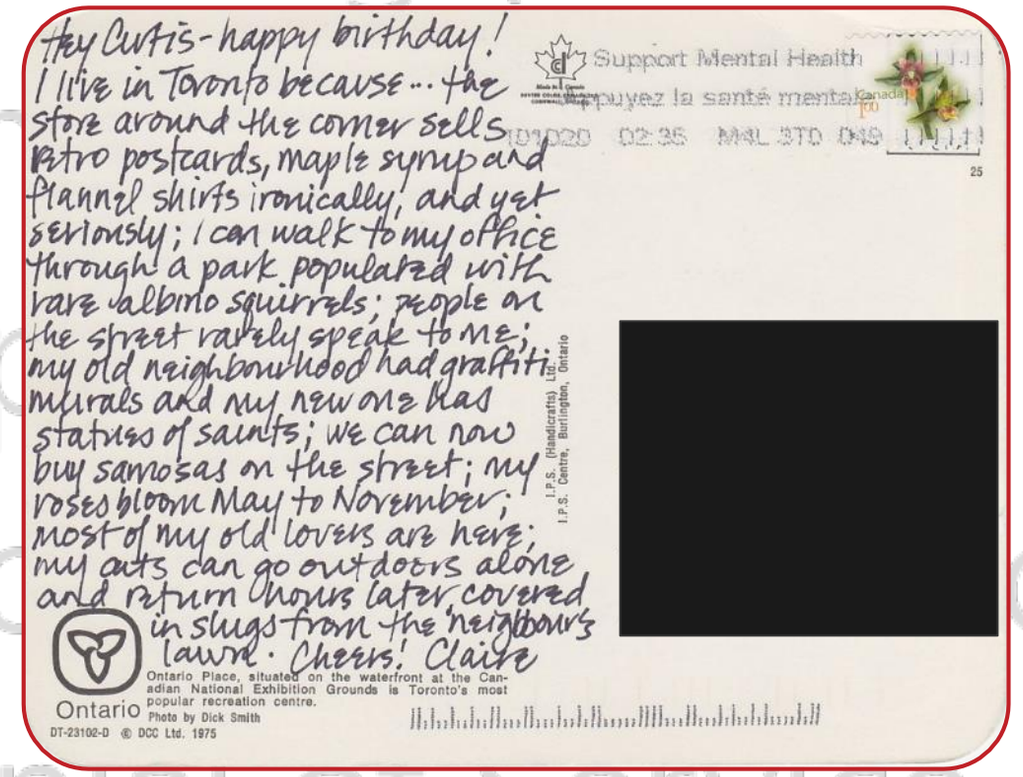


Information Disclosure

Framing questions:

- Can somebody else look at the data being transmitted?
- Can unauthorized users access the data on disk (data at rest)?
- Can unauthorized users infer valuable information from errors in the system?

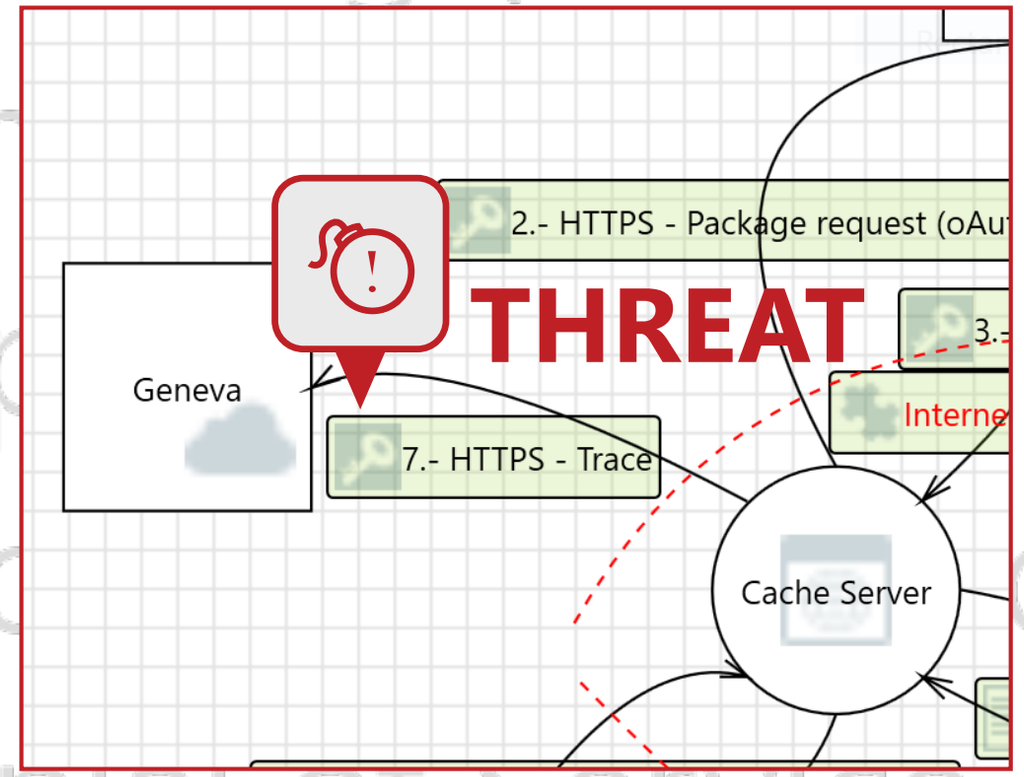
Spoofing (of user ide
Tam
Rep
Info osur
Denial of Service (Do
Elevation of Privilege



Information Disclosure

Information in logs might be Disclosed to an interloper en route to Geneva.

How can Cache Server keep this information secret?



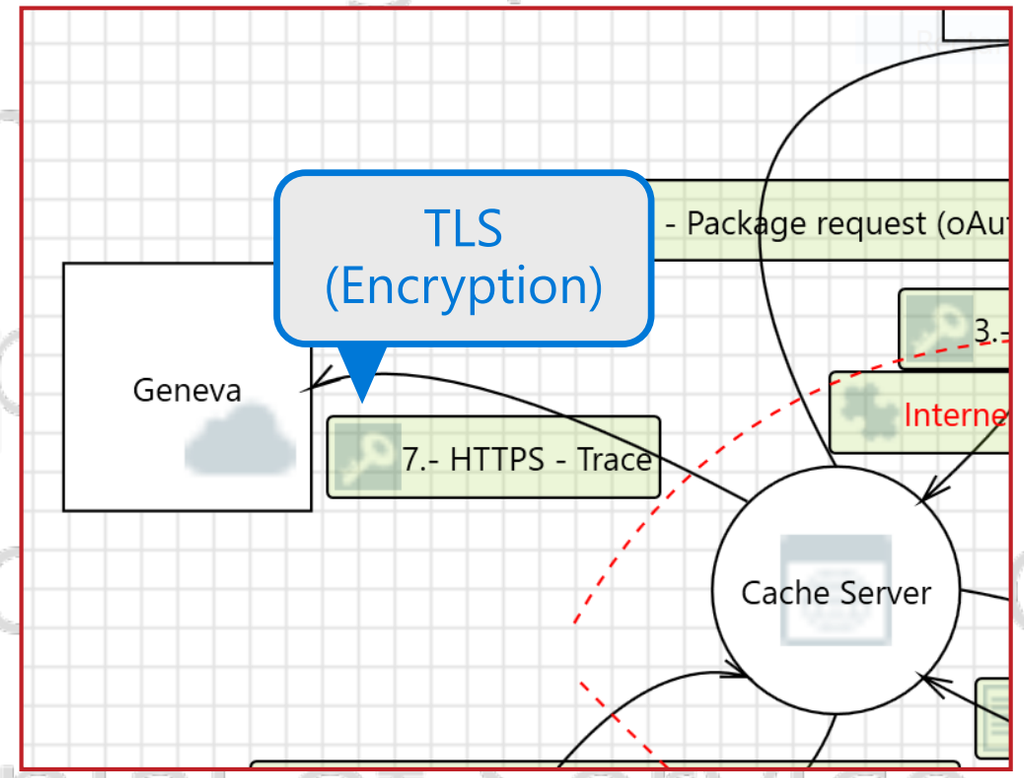
Spoofing (of user ide
Tar
Rep
Info
osur
Denial of Service (Do
Elevation of Privilege

Information Disclosure

How do we mitigate?

- Encryption in transit (i.e. HTTPS)
- Encryption at rest
- Security details must not be exposed in error messages

*Transport Layer Security (TLS)



Denial of service

Framing questions:

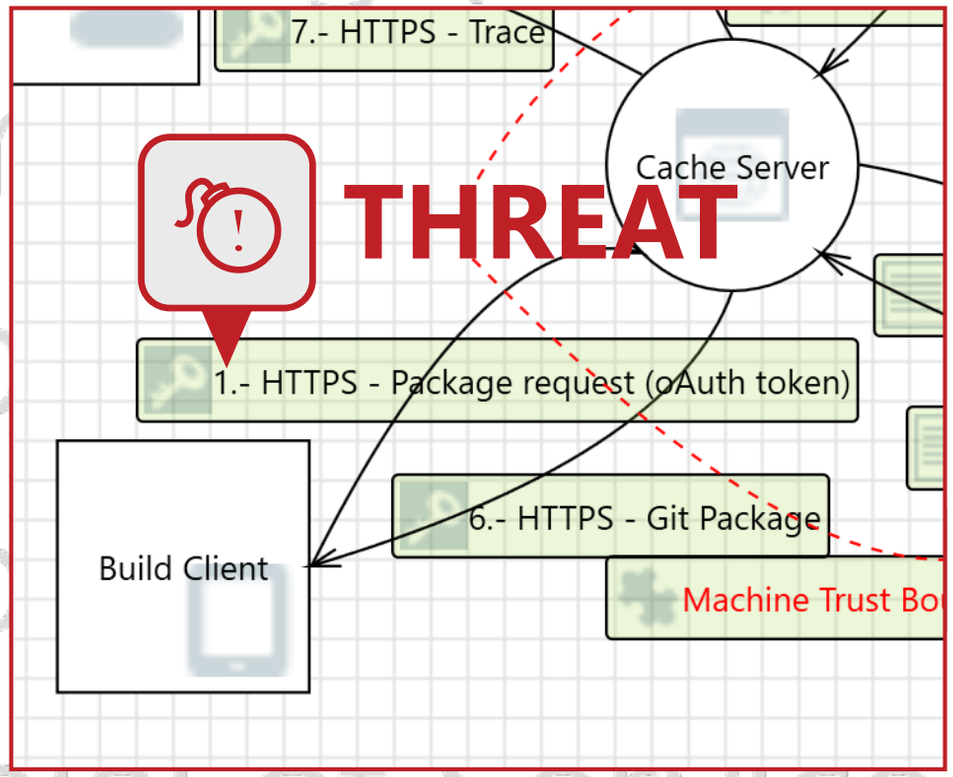
- Could somebody prevent this interaction from being established?
- Could service disruption occur by using/abusing the API?

Spoofing (of user iden
Ta
Re
In sur
Denial of Service (Do
Elevation of Privilege

Denial of service

What if a hostile Build Client floods the Cache Server with requests?

Could the Build Client DOS the Cache Server by running it out of disc cache?

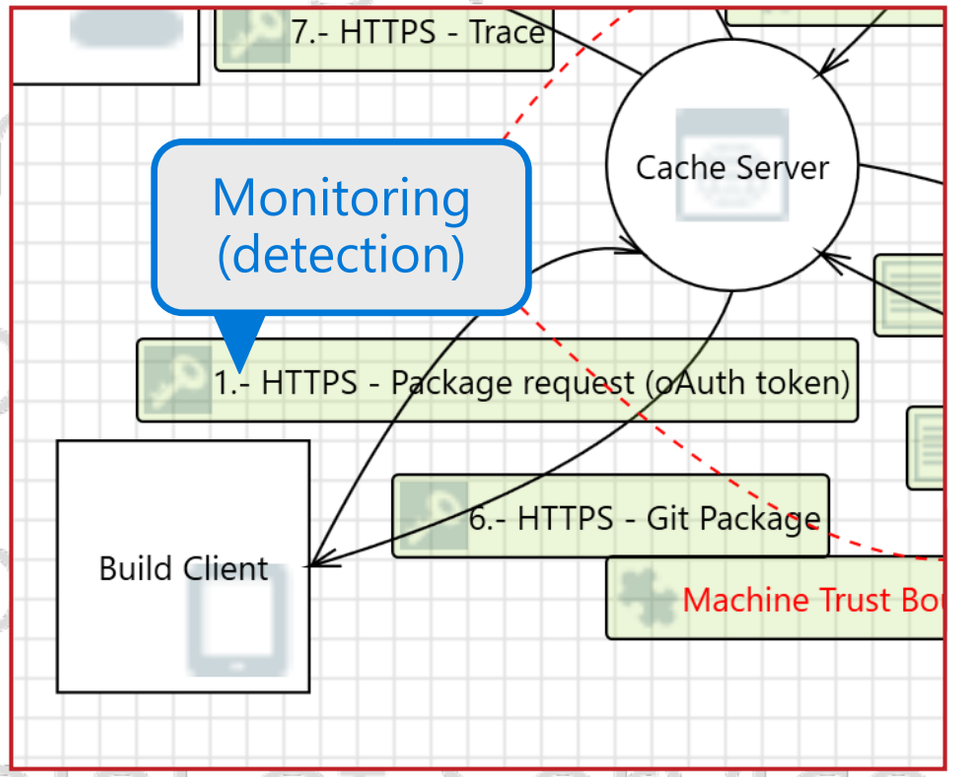


Spoofing (of user ide
Tam
Rep
Info
osur
Denial of Service (Do
Elevation of Privilege

Denial of Service

How do we mitigate?

- Azure DoS protection
- Monitor service availability
- Throttling



Spoofing (of user ide
Tam
Rep
Info
osur
Denial of Service (Do
Elevation of Privilege

Elevation of Privileges

Framing questions:

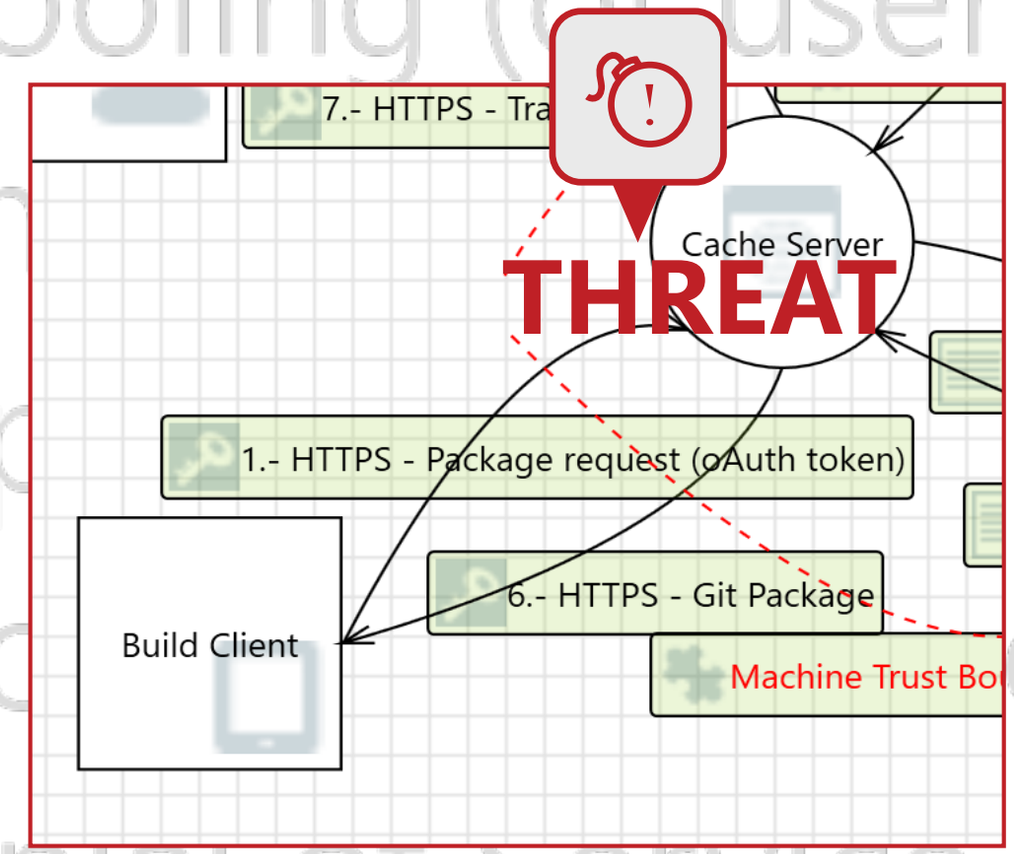
- Can the user do more than they are supposed to?
- What else does your process have permission to do?

Spoofing (of user ide
Tam
Rep
Info osur
Denial of Service (Do
Elevation of Privilege

Elevation of Privileges

Could an attacker Elevate to the Cache Server's Privileges and gain additional access to VSTS?

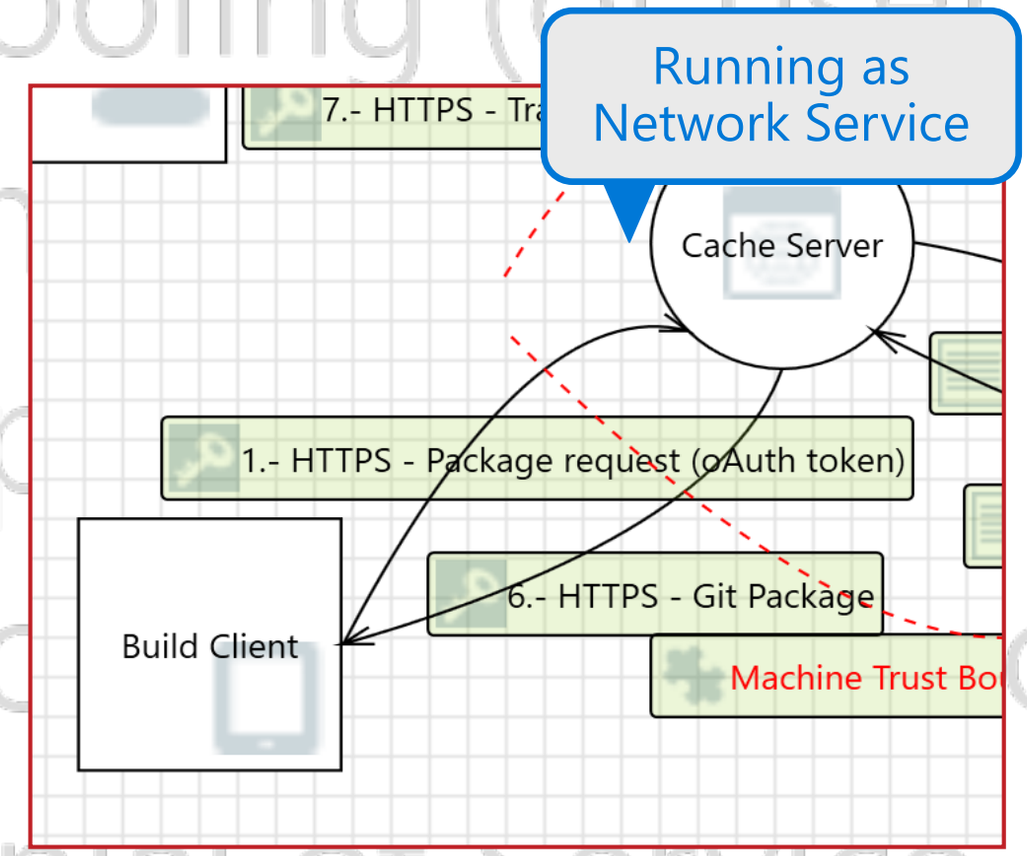
Could a malformed package request let a rogue Build Client get the Cache Server to do things other than what it was designed to do?



Elevation of Privileges

How do we mitigate?

- Run services with limited privileges
  i.e., Network Service
- Strong access control policies and procedures
- Treat user input as hostile



Model analysis

STRIDE represents these threat categories:

Spoofing (of user identity)
Tampering
Repudiation
Information Disclosure (privacy breach or data leak)
Denial of Service (DoS)
Elevation of Privilege

Key Takeaways

Threat model = Dataflow diagram (DFD) + model analysis

Build a model for the right reason: to uncover risks & bugs

Build your dataflow diagram (DFD)& then analyze (STRIDE)

Part 2: Microsoft Threat Modeling Tool

https://aka.ms/threatmodelingtool

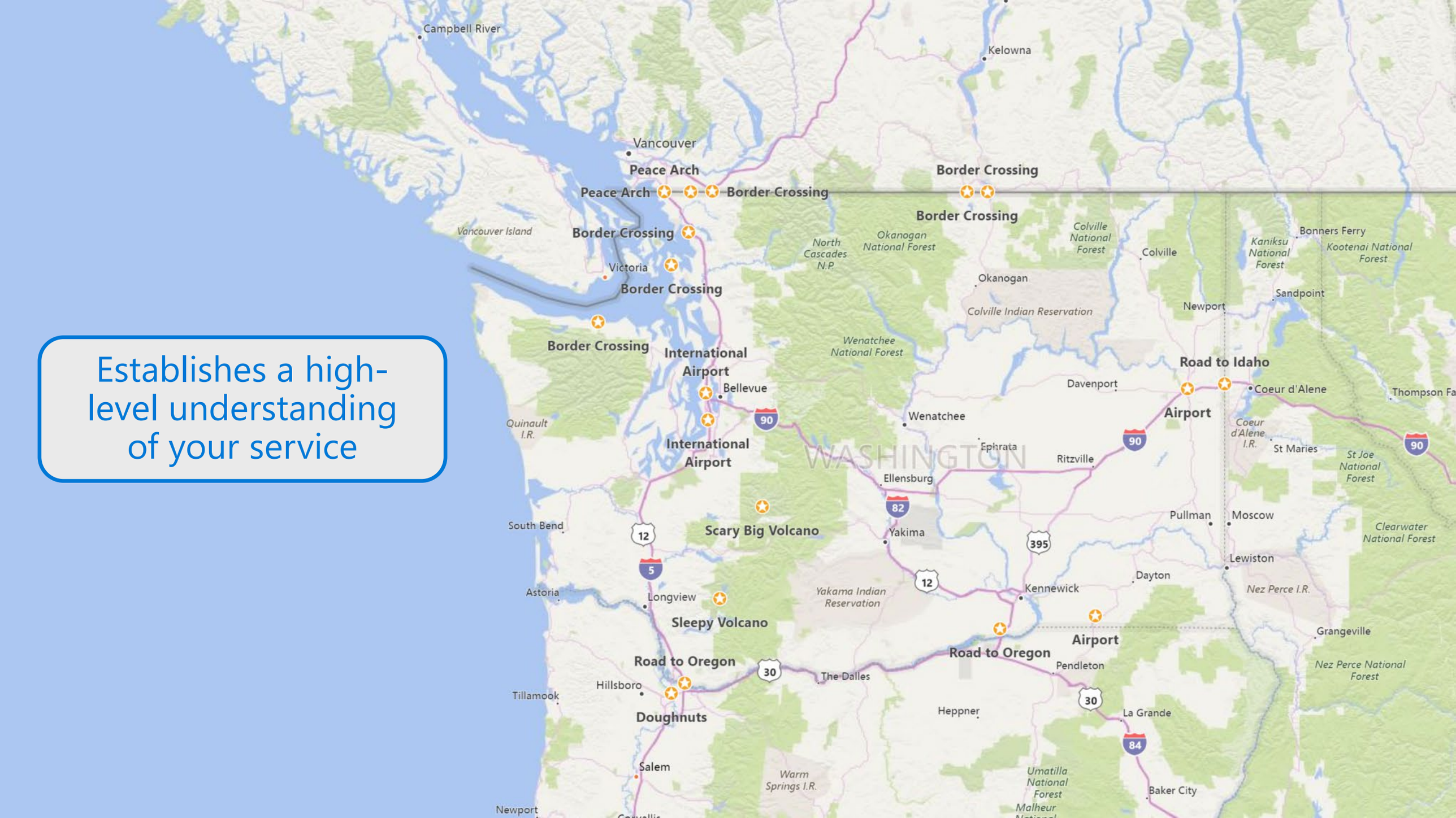
Now it is https ^^^^^^^ ☺

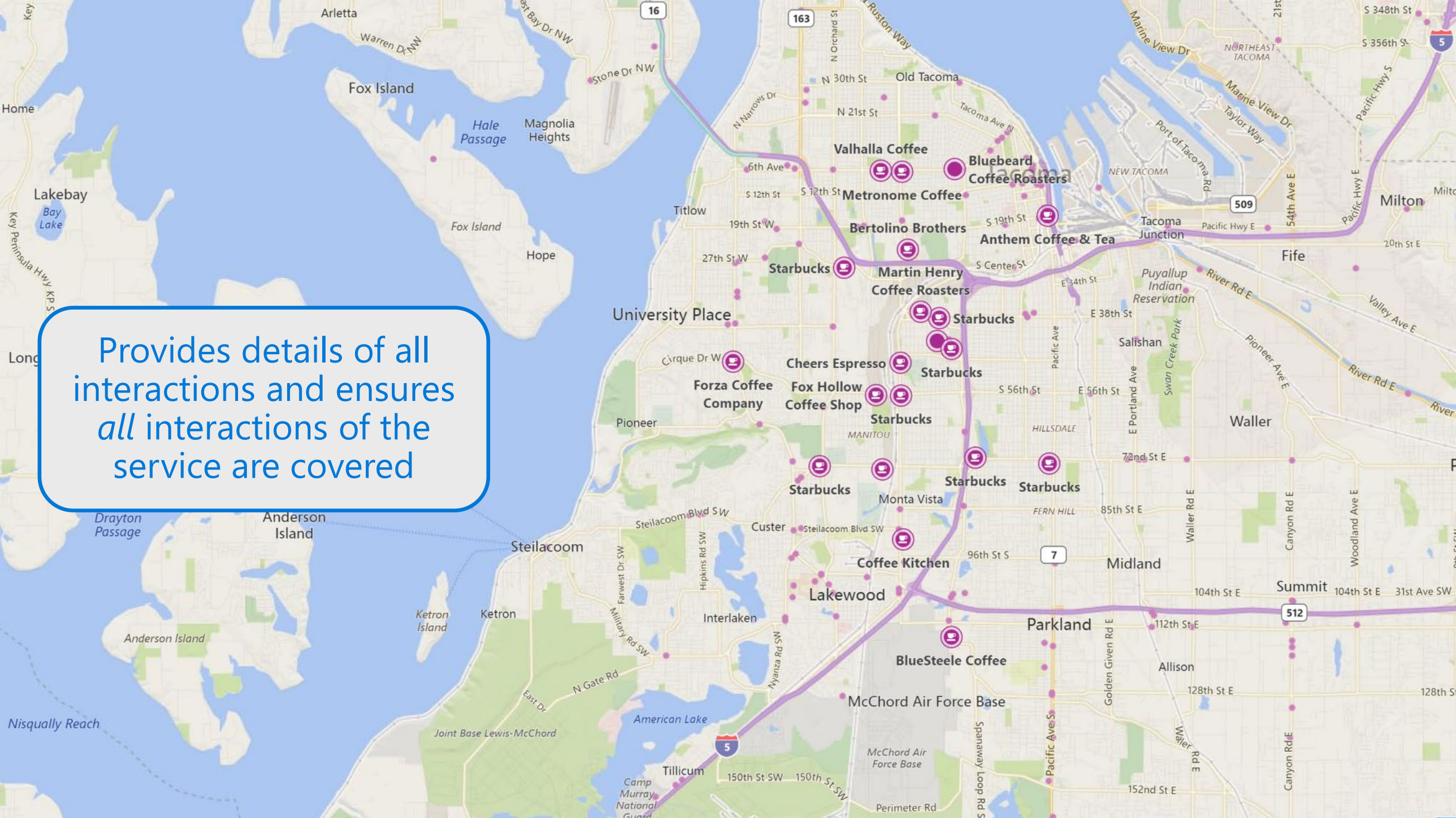
Threat modeling tool overview

- Smart diagram objects
- Smart threats
- Threat and mitigation output
- Self-contained, stand-alone tool
- Ideal for services, applications, and OS
- Not designed for modeling hardware

It’s all in the details


Peace Arch
Peace Arch
Border Crossing
Border Crossing
Border Crossing
Border Crossing
Border Crossing
Border Crossing
Border Crossing
International Airport
International Airport
Scary Big Volcano
Sleepy Volcano
Road to Oregon
Doughnuts
Road to Oregon
Airport
Road to Idaho
Airport

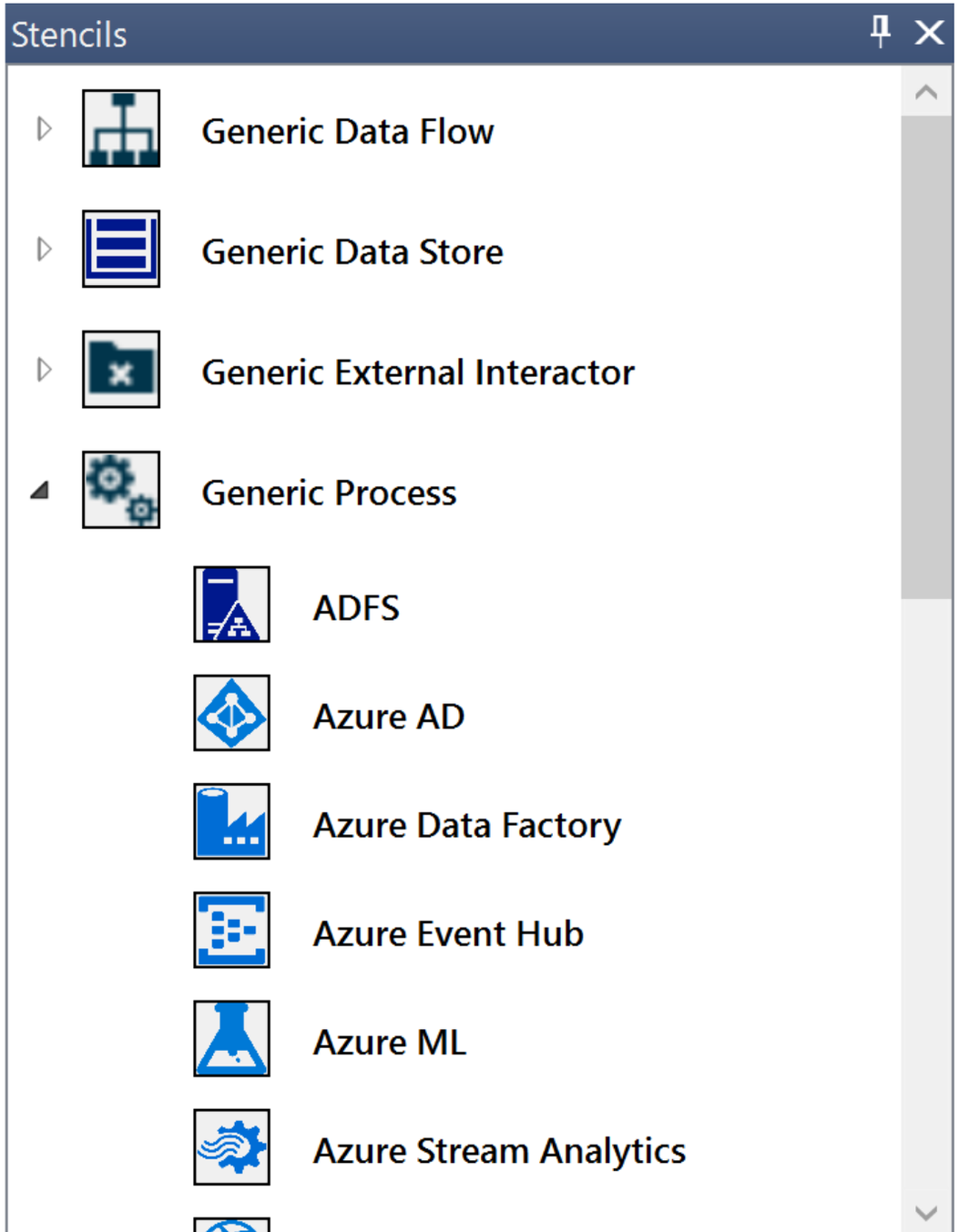

Establishes a high-level understanding of your service
Campbell River
Kelowna
Vancouver
Peace Arch
Peace Arch
Border Crossing
Border Crossing
Vancouver Island
Border Crossing
Victoria
Border Crossing
Border Crossing
Border Crossing
International Airport
Bellevue
International Airport
Quinault I.R.
South Bend
Scary Big Volcano
Astoria
Longview
Sleepy Volcano
Road to Oregon
Hillsboro
Tillamook
Doughnuts
Salem
Newport
Warm Springs I.R.
Yakama Indian Reservation
Wenatchee
Ephrata
Ellensburg
Yakima
Ritzville
WASHINGTON
Heppner
The Dalles
Pendleton
Road to Oregon
Airport
Kennewick
Dayton
Pullman
Moscow
Lewiston
Nez Perce I.R.
Grangeville
Nez Perce National Forest
Clearwater National Forest
La Grande
Baker City
Umatilla National Forest
Malheur
Wenatchee National Forest
North Cascades N.P.
Okanogan National Forest
Colville National Forest
Colville
Okanogan
Colville Indian Reservation
Newport
Bonners Ferry
Kaniksu National Forest
Kootenai National Forest
Sandpoint
Davenport
Road to Idaho
Airport
Coeur d'Alene
Coeur d'Alene I.R.
St Maries
St Joe National Forest
Thompson Fa
90
82
395
12
5
30
84


Provides details of all interactions and ensures *all* interactions of the service are covered
Valhalla Coffee
Bluebeard Coffee Roasters
Metronome Coffee
Bertolino Brothers
Anthem Coffee & Tea
Starbucks
Martin Henry Coffee Roasters
Starbucks
Cheers Espresso
Starbucks
Forza Coffee Company
Fox Hollow Coffee Shop
Starbucks
Starbucks
Starbucks
Starbucks
Coffee Kitchen
BlueSteele Coffee
Arletta
Fox Island
Hale Passage
Magnolia Heights
Lakebay
Bay Lake
Hope
Titlow
University Place
Old Tacoma
Tacoma
Tacoma Junction
Milton
Fife
Puyallup Indian Reservation
Salishan
Waller
Pioneer
Custer
Monta Vista
Steilacoom
Anderson Island
Drayton Passage
Ketron
Ketron Island
Interlaken
Lakewood
Midland
Parkland
Summit
Allison
McChord Air Force Base
American Lake
Joint Base Lewis-McChord
Tillicum
Nisqually Reach
Marine View Dr
Pacific Hwy E
Pacific Hwy S
Taylor Way
Port of Tacoma Rd
Tacoma Ave N
N 30th St
N 21st St
6th Ave
S 12th St
19th St W
27th St W
S 19th St
S Center St
E 34th St
E 38th St
Cirque Dr W
Steilacoom Blvd SW
S 56th St
E 56th St
72nd St E
85th St E
96th St S
104th St E
112th St E
128th St E
150th St SW
152nd St E
Perimeter Rd
River Rd E
Valley Ave E
Pioneer Ave E
Waller Rd E
Canyon Rd E
Woodland Ave E
Golden Given Rd E
Spanaway Loop Rd S
Pacific Ave S
Military Rd SW
Nyanza Rd SW
Hipkins Rd SW
Farwest Dr SW
N Gate Rd
East Dr
Camp Murray National Guard
McChord Air Force Base
NORTHEAST TACOMA
NEW TACOMA
HILLSDALE
MANITOU
FERN HILL
Swan Creek Park
E Portland Ave
Pacific Ave
54th Ave E
509
512
7
5
16
163

Stencils

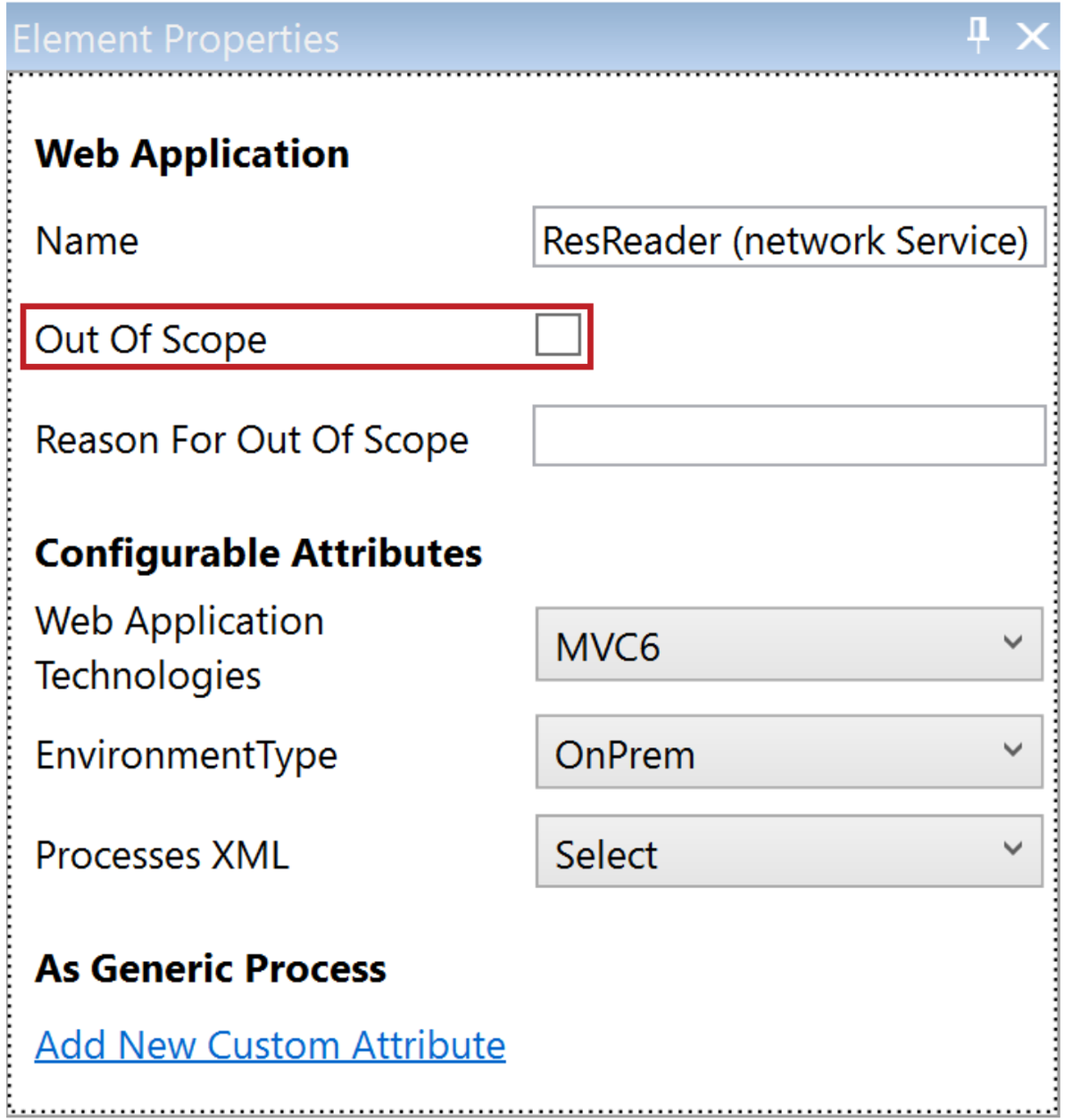
Objects to drag into a threat model

- Processes
- External entities
- Data stores
- Data flows
- Trust boundaries

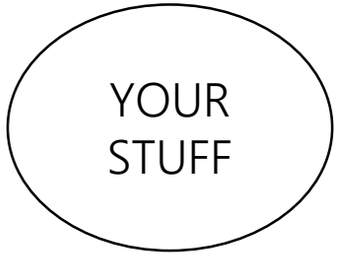


Properties

- Characteristics of selected entity (stencil)
- Specific to the type of entity
- Ex. HTTP dataflow vs HTTPS dataflow



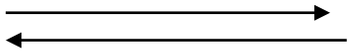
Dataflow diagram elements



Circles: your service and processes
(i.e. your code or under your control)

Squares: external interactors (users, 3rd party services
and other Microsoft services not under your control)

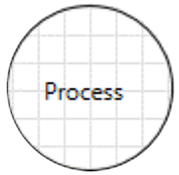
Lines: data storage
(databases, Azure storage, shared files)



Arrows: data, control, and influence move between elements

Dashed Lines: privilege boundary

Dataflow diagram stencils



Azure AD

Azure Web job

Dynamics CRM

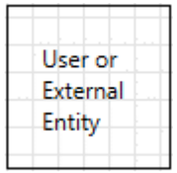
Azure ML

WCF

Web API

Web Application

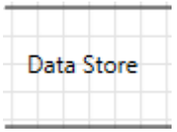
Etc.



Mobile Client

Web browser

Anything external to the system that you can't control

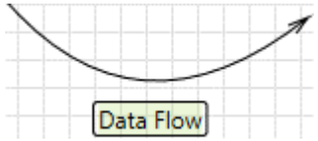


Database

Cached

Azure DocDB

Azure Storage

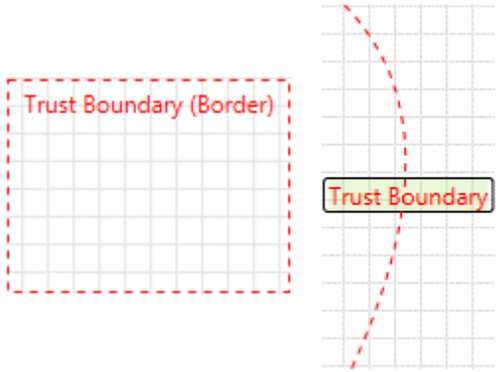


Request or Response

Network traffic

Function call

Any flow where data moves from one entity to another entity on DFD



Points/surfaces where an attacker can interject

Examples of boundaries:

Machine

Privilege

Network (even TLS)

Microsoft Threat Modeling Tool Demo

Microsoft Threat Modeling Tool Links

- TM Templates are available on our GitHub repo, we invite you all to collaborate: https://aka.ms/tmtrepo

- We are always looking for feedback, so please provide that using this link: https://aka.ms/threatmodelingsurvey

Key Takeaways

All-in-one tool for creating dataflow diagram & analysis.

Use “design view” to create level 0 dataflow diagram.

Use “analysis view” to conduct STRIDE.

Go Do

- ✓ Own a service?
  Start threat modeling it!
- ✓ Working on a new version of a service?
  Great! Start modeling the new design!
- ✓ My service is already in production.
  Go ahead and model everything as-is!
- ✓ I don't own a service.
  Go talk to your PM/Dev/OPS counterpart about how you can help.

Q&A

I will be doing a QA later from 2:00-2:45 , come talk if you have questions ☺

- ✓ Security community
- ✓ Documentation
- ✓ Training resources
- ✓ Event content
- ✓ And more…

Your online STRIKE resource

Visit STRIKE Central at //STRIKE

strike

Thank you!