

# **CMGT431**

## **Week 1 Assignment**

### **Create DFD in Microsoft TMT**

**Tom Olzak, MBA, CISSP**

Online Faculty

University of Phoenix

February 2016

# Overview

- Keep it simple
- Not a tool used by security professionals
- Use only icons provided by the tool
- Set attributes

# Data Flow Diagrams

- Show flow of information between components in a system
- Useful for developers to set authentication and ensure trust between components
- Useful for security professionals to understand the information flowing and where it flows
- DFDs do not replace attack trees
- Attack trees in Week 2
- For how we apply these concepts, see ***Practical Application of Threat Modeling*** in **Student Materials** for this activity

# MICROSOFT THREAT MODELING TOOL 2016

## Threat Model:

### Create A Model

Model your system by drawing diagram(s). Make sure you capture important details.

### Open A Model

Open an existing model and analyze threats against your system; do not worry, the tool will help you identify them.

### Getting Started Guide

A step-by-step guide to help you get up and running now.

## Template For New Models

SDL TM Knowledge Base (Core)(4.1.0.9)

Browse...

## Recently Opened Models

[Sample Threat Model.tm7](#)

## Threat Modeling Workflow

1. Select your template.
2. Create your data flow diagram model.
3. Analyze the model for potential threats.
4. Determine mitigations.

## Template:

### Create New Template

Define stencils, threat types and custom threat properties for your threat model from scratch.

### Open Template

Open an existing Template and make modifications to better suit your specific threat analysis.


## Template Workflow


Use templates to define threats that applications should look for.


1. Define stencils
2. Define categories
3. Define threat properties
4. Define threat
5. Share your template





Stencils


 Web Application


 Web Service


 Virtual Machine


 Applications Running on a non

 Generic External Interactor

 Browser

 Authorization Provider

 External Web Application

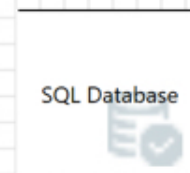
 External Web Service

Element Properties

[Add New Custom Attribute](#)



Diagram 1 X





- Web Server
- Windows Store Process
- Win32 Service
- Web Application
- Web Service
- Virtual Machine
- Applications Running on a non-OS

**Element Properties**

Reason For Out Of Scope

**Redefined Static Attributes**

Code Type

**Configurable Attributes**

**Is Generic Process**

Running As

Isolation Level

Accepts Input From

Implements or Uses an Authentication Mechanism

Implements or Uses an Authorization Mechanism

Standard User With Elevation

Standard User Without Elevation

Windows Store App

# Web Application Attributes

Element Properties

**Configurable Attributes**

**As Generic Process**

Running As	Administrator
Isolation Level	Not Selected
Accepts Input From	Any Remote User or Entity
Implements or Uses an Authentication Mechanism	Yes
Implements or Uses an Authorization Mechanism	No
Implements or Uses a Communication Protocol	Yes
Sanitizes Input	No
Sanitizes Output	Not Selected

[Add New Custom Attribute](#)



# SQL Server Attributes

Element Properties 

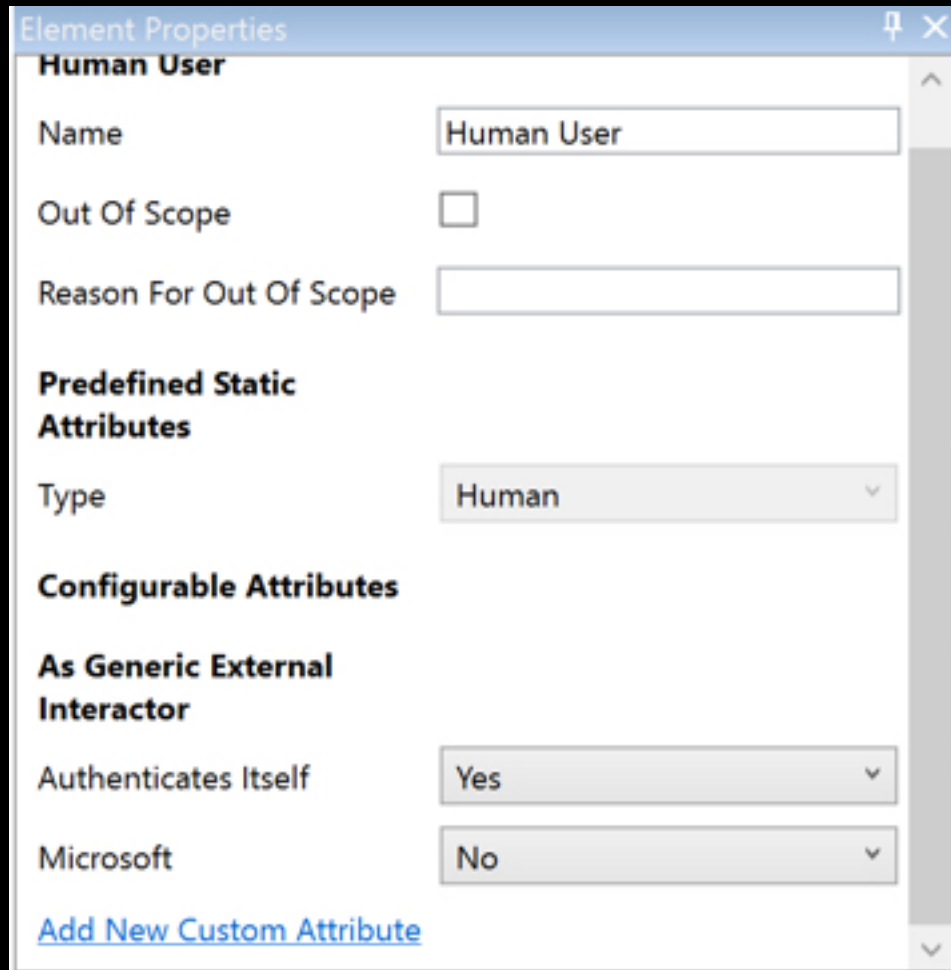
Store type SQL Relational Database

**Configurable Attributes**

**As Generic Data Store**

Stores Credentials	Yes
Stores Log Data	Yes
Encrypted	No
Signed	No
Write Access	Yes
Removable Storage	No
Backup	Yes
Shared	Yes

# Human Attributes



The image shows a software window titled "Element Properties" with a standard Windows-style title bar (minimize, maximize, close buttons). The window is divided into several sections for configuring a "Human User".

**Human User**

Name: Human User

Out Of Scope: ☐

Reason For Out Of Scope:

**Predefined Static Attributes**

Type: Human

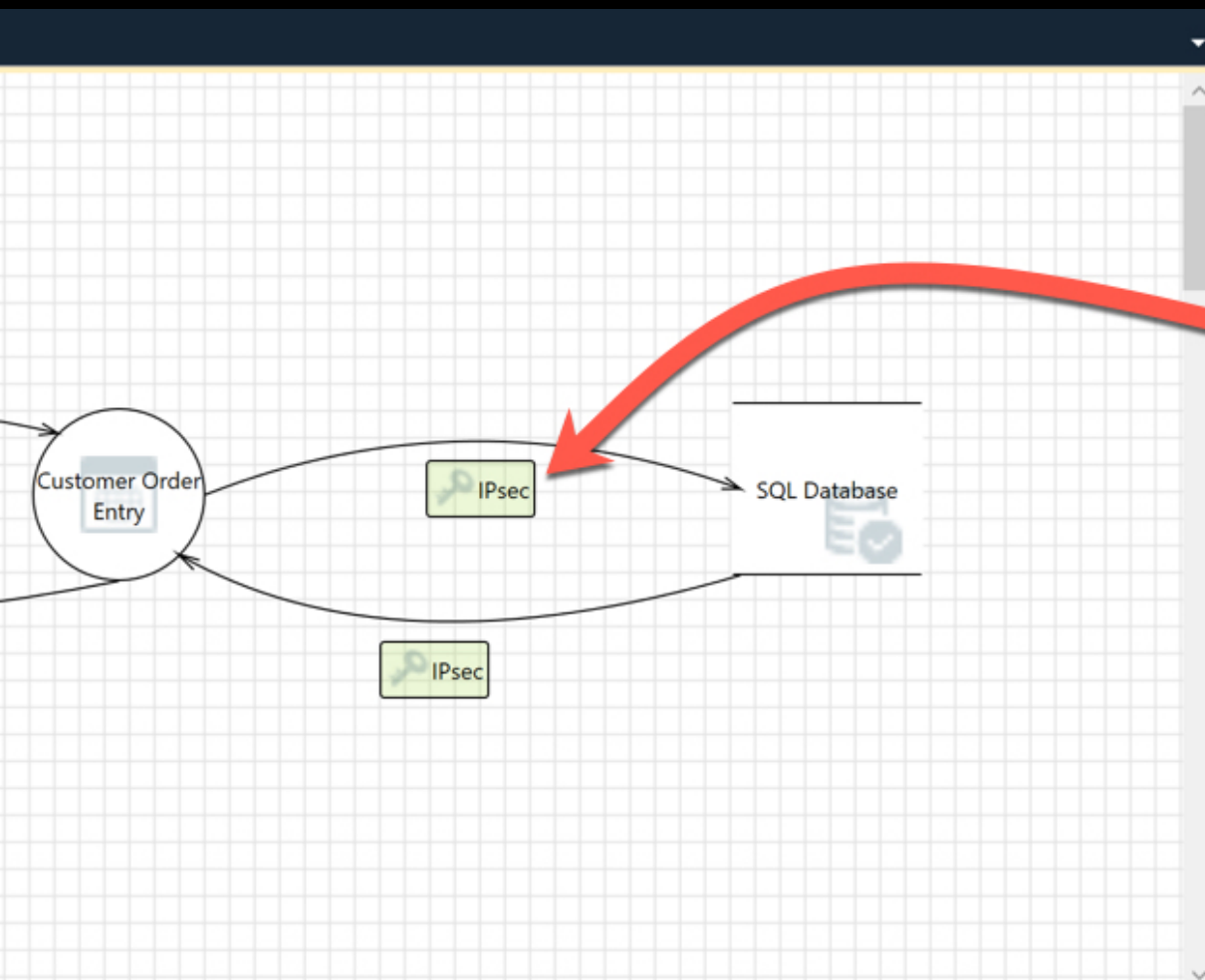
**Configurable Attributes**

**As Generic External Interactor**

Authenticates Itself: Yes

Microsoft: No

[Add New Custom Attribute](#)



**Stencils**

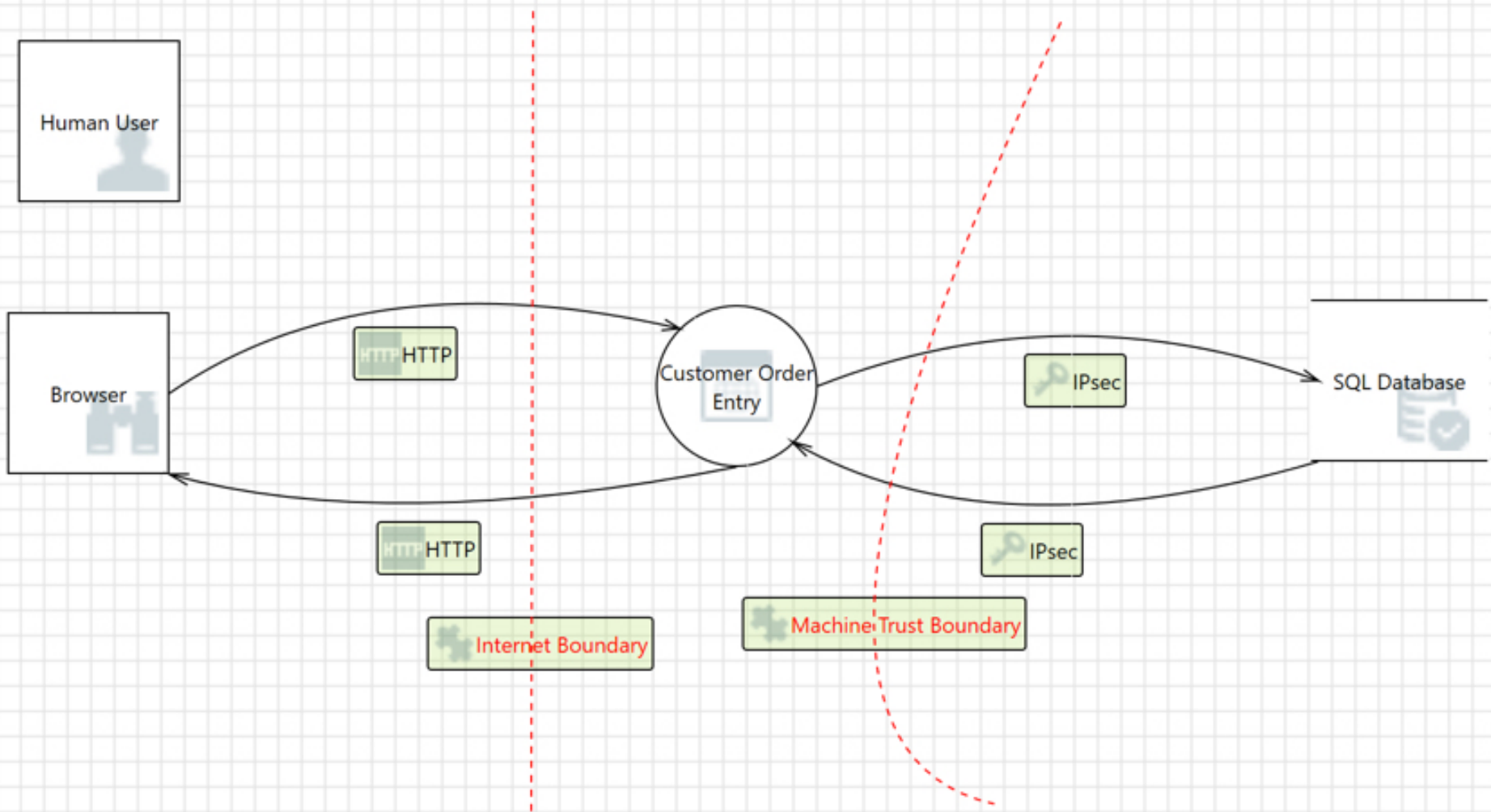
- Generic Data Flow
  - HTTP
  - HTTPS
  - Binary
  - IPsec**
  - Named Pipe
  - SMB
  - RPC or DCOM
  - ALPC

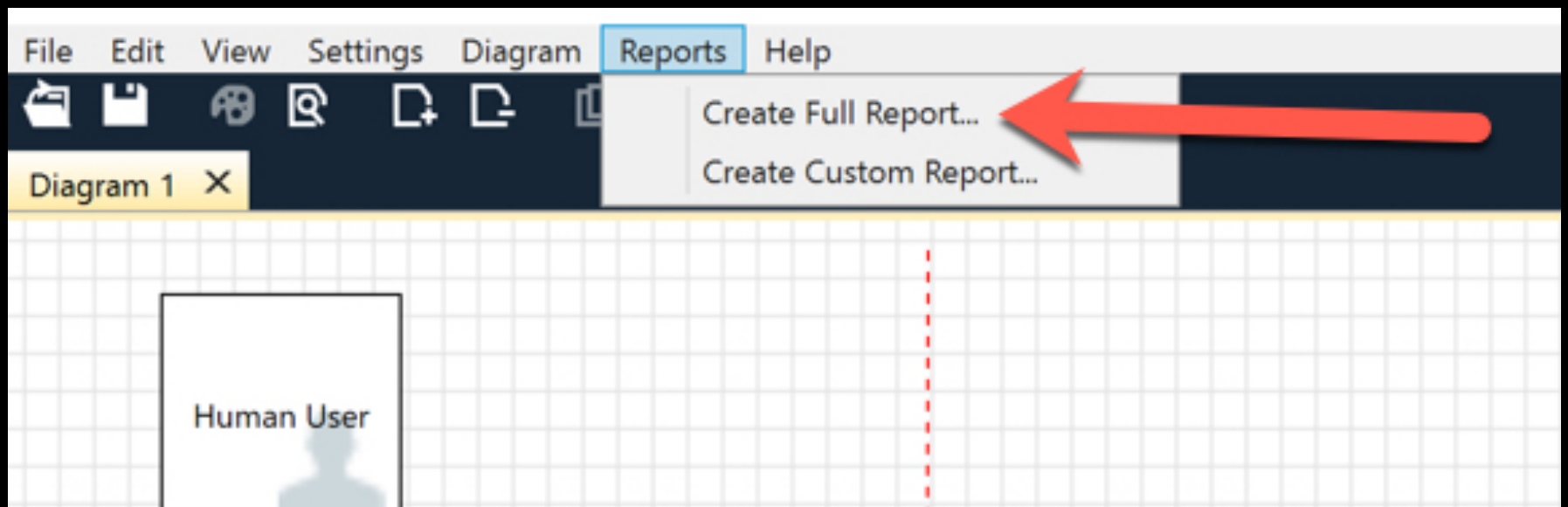
**Element Properties**

**Diagram**

Name:

[Add New Custom Attribute](#)





# Closing Comments