Student Name:	Section:	Date:

Activity 3
Threat Modeling

Instructions/Directions:

Be able to create a "Threat Model" of your developed Web Application using various threat modeling methodologies and tools. Generate a threat model report using the Threat Modeling tools (MS SDL Threat Model or OWASP Threat Dragon).

Show proof of your activity completion by providing clear screenshot of your entire desktop environment based on the tasks performed. Screenshot must be included in the activity template provided in MS Teams Assignment.

Submission Note (Individual Activity)
Use the Activity template attached in MS Teams Assignment.
Use file name convention (LASTNAME_CTINASSL_SECTION_TERM_AY_Activity3.pdf).
Submit a PRINTED document and upload the Softcopy (PDF file) in MS Teams
Submit OWASP ZAP HTML Generated Report File

Student Name:	Section:	Date:

THREAT MODELING

Threat Model is usually a visual representation with documentation explaining each process and any threats associated with it.

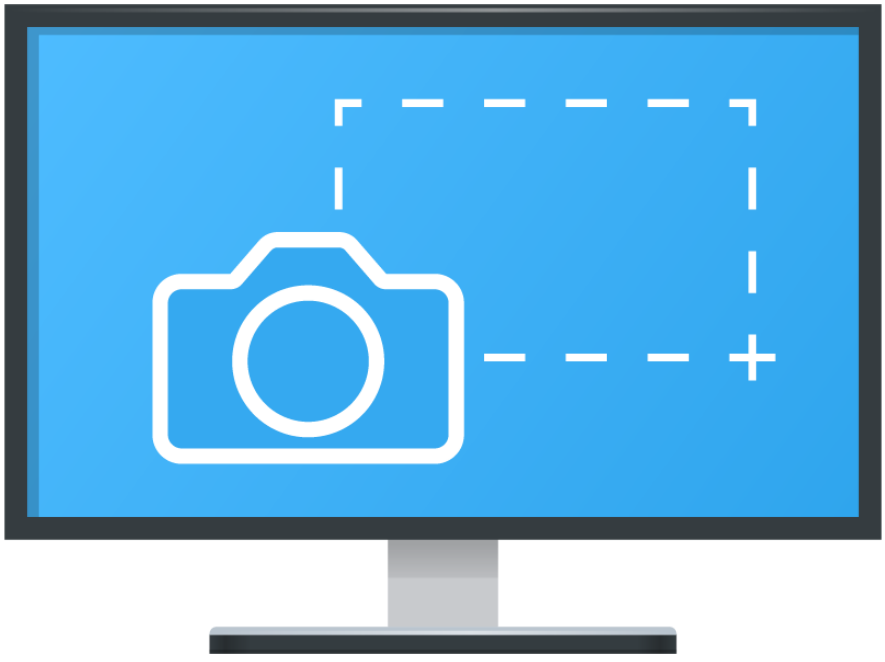
IDENTIFYING SECURITY OBJECTIVES

The initial step in the threat modeling example is to gather as much background information as possible.

Business Case	Description
Company and Industry	
Solution Requirements	
Compliance Requirements	
Quality of Service Requirements	
Assets	
Team	
Security Objective	

CREATE AN APPLICATION OVERVIEW

In this step, you outline what your Web application does. Your goal is to identify your application's key functionality, characteristics, and clients. Draw a rough diagram that describes the composition and structure of your application, its subsystems, and its deployment characteristics.

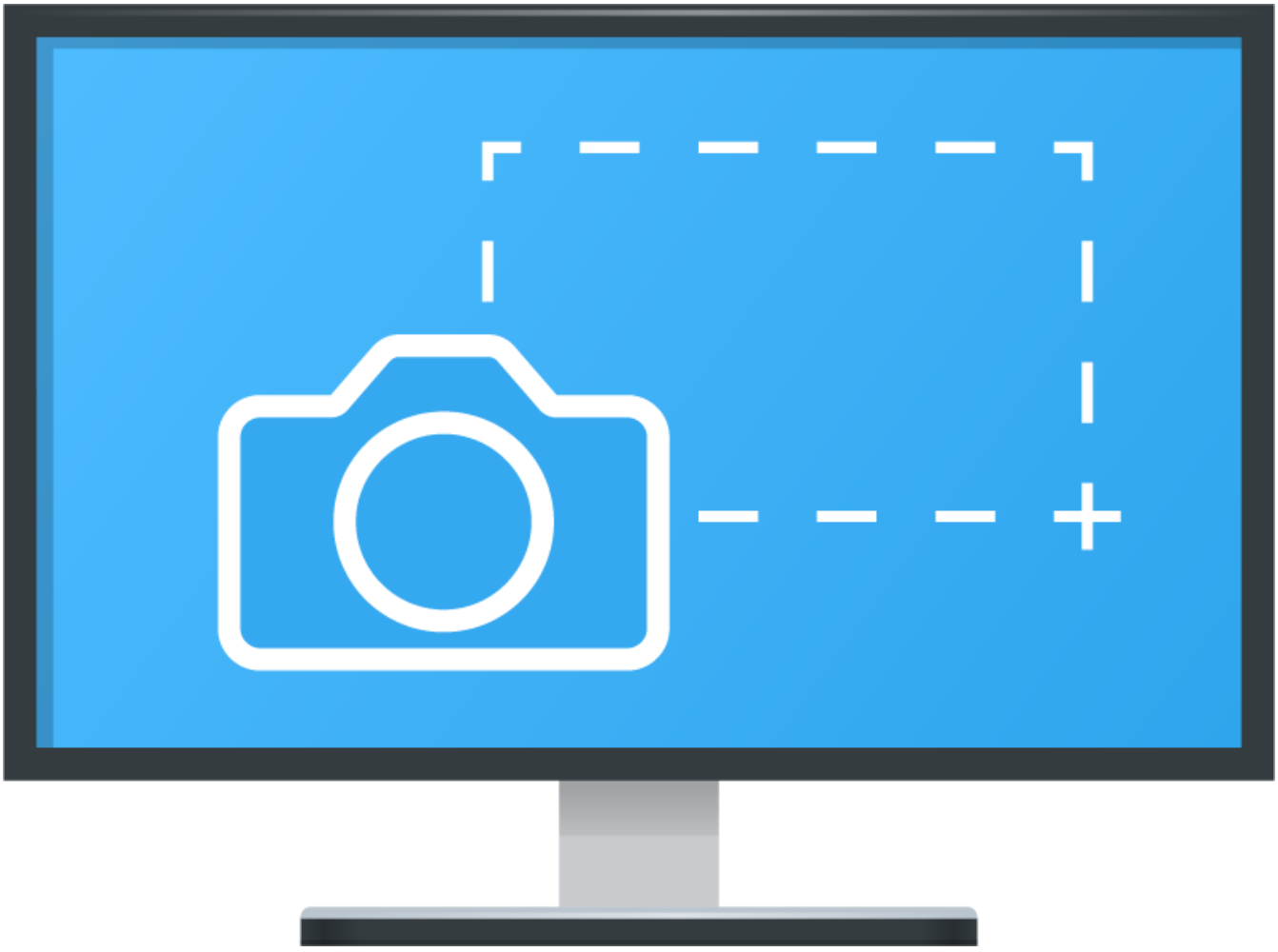


System Architecture

Application Overview	Description
Roles	
Key Usages	
Technologies	
Security Mechanism	

DECOMPOSE YOUR APPLICATION

In this step, you break down your application to identify trust boundaries, data flows, entry points, and exit points. The more you know about the mechanics of your application, the easier it is to uncover threats and discover vulnerabilities. Architectural diagrams and overviews of the proposed application design help in creating a DFD.



Data Flow Diagram

IDENTIFY THREATS AND VULNERABILITITES

In this step, you identify threats and attacks that might affect your application and compromise your security objectives. These threats are the bad effects that could happen to your application. STRIDE methodology introduced by Microsoft can be used to identify threats. As a next step, STRIDE threat modeling against each component (known as component-based STRIDE threat modeling) can be performed.

RATE AND PRIORITIZE THREATS

DREAD methodology is used to rate, compare, and prioritize the severity of risk presented by each threat that is classified using STRIDE. To determine the ranking of a threat, the threat analyst must answer basic questions for each factor of risk.

IDENTIFY COUNTERMEASURES AND MITIGATIONS

Once threats have been identified, compared, and prioritized using threat modeling method it is time to define countermeasures to those threats. Note that countermeasures to threats can also be called security requirements or threat mitigations.

Student Name:	Section:	Date:

Criteria	Activity Rubrics					Points
	Not Attempted (0 points)	Beginning (1 point)	Developing (2 points)	Proficient (3 points)	Exemplary (4 points)	
Asset Identification	No assets identified.	Few assets identified; unclear or incorrect descriptions and values.	Some assets identified, but descriptions and values are unclear.	Most assets identified with minor details missing.	All assets identified with detailed descriptions and value assessment.	
Data Flow Diagram (DFD) Creation	No DFD created.	Major inaccuracies in representation of data flows.	DFD incomplete or with significant inaccuracies in data flows or interactions.	DFD mostly complete; minor details missing.	Detailed DFD created, accurately representing all data flows and interactions.	
Threat Identification, Analysis, Prioritization and Mitigation Strategies	No severity classification	Few threats identified; major gaps in threat identification.	Some threats identified but key threats missing.	Most potential threats identified with minor omissions.	Comprehensive threat identification using a framework (e.g., STRIDE), covering all potential threats.	
	No attempt to analyze and prioritize threats.	Threats not prioritized or incorrectly assessed.	Some threats analyzed; prioritization unclear or incomplete.	Most threats analyzed and prioritized with minor inconsistencies.	Thorough analysis and prioritization based on impact and likelihood, using a structured methodology.	
	No mitigation strategies proposed.	Proposed mitigation strategies proposed are ineffective.	Mitigation strategies proposed for some threats, with significant gaps.	Mitigation strategies proposed for most threats, with minor gaps in coverage.	Detailed mitigation strategies proposed for all threats, covering technical, procedural, and design controls.	
Risk Assessment	No recommendations for remediation.	Little to no risk assessment; risk levels missing or inaccurate.	Some threats assessed; risk levels assigned but with inconsistencies.	Most threats assessed with risk levels, minor inaccuracies in assessment.	Comprehensive risk assessment completed, with risk levels assigned for all threats accurately.	
Reporting and Documentation	No documentation provided.	Poor or incomplete documentation with missing key information.	Basic documentation provided with several gaps or omissions.	Documentation mostly complete with minor omissions	Thorough and well-organized documentation of all steps, findings, and decisions. .	

Total Score and Feedback			**TOTAL POINTS EARNED**	
☐ Exemplary	20	Task was completed with exceptional accuracy and thoroughness, covering all necessary steps without issues.		
☐ Proficient	16-19	Task was completed well, with minor issues that were resolved.		
☐ Developing	12-15	Task was completed with significant issues or errors, partially resolved.		
☐ Beginning	8-11	Task was not completed correctly, with major issues or unresolved errors.		
☐ Not Attempted	0-7	Task was not completed correctly.		

Evaluated by: _____ Name of Course Instructor/Date	**Remarks/Comments**