National College of Ireland

Embrace Threat Intelligence into Threat Modelling for preventing potential vulnerabilities.

MSc Research Project
Cyber Security

Alekhya Nannapaneni
Student ID: X21233896

School of Computing
National College of Ireland

Supervisor: Mr. Michael Prior

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ……Alekhya Nannapaneni……

Student ID: ……X21233896……

Programme: ……M.Sc Cyber Security…… **Year:** ……2023…..

Module: ……M,Sc Research Project ……

Supervisor: ……Michael Prior……

Submission Due Date: ……14/08/2023…..

Project Title: Embrace Threat Intelligence into Threat Modelling for preventing potential vulnerabilities.

Word Count: …….. **Page Count**……23……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Alekhya……

Date: ……14/08/2023……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Abstract

In the real-world cyber criminals are finding new technologies and techniques to attack on the different organizations like health sectors, educational institutions, government sectors, information technologies. This causes huge loss of data, compromise sensitive information loss, services downtime, ransomware. Hackers can also use this information to cause financial loss. To face these consequences and mitigate the attacks organizations should be well prepared. In order to perform this, we should be updated and have a understanding of the emerging threats and patterns. This knowledge helps to develop the defense mechanisms. The objective of this assessment is to highlight the importance of analyzing the real time threats along with threat modelling and explaining the integration advantages in a practical manner. Here, our main objective is to predict vulnerabilities or threats for the application defined. The framework consists of three primary steps: preparing an architectural diagram for analysis, threat modelling for risk assessment report, and processing a dataset for threat intelligence report. Threat intelligence reports will be analyzed to determine which are specific to architecture components and merge with threat modelling reports. The baseline Common Vulnerability Scoring System (CVSS) score mentioned are updated using the insights of the report generated. This helps in having more accurate data for finding possible vulnerabilities. This also gives an idea of threat patterns and suggestions for mitigations. The results obtained include vulnerabilities security misconfiguration, directory traversal remote code execution, improper input validation with the severities 9.8 (Critical), 8 (High), 3.9 (Low). The remediation measures in general include performing proper input validation for Unicode characters, updating the software versions, verify unauthorized access.

Link to video presentation: https://studentncirl-my.sharepoint.com/:v:/g/personal/x21233896_student_ncirl_ie/ETFmjdozbfRPpS7mUs44x6oBGN2sqnVjjR3CnMIBw3bxvA?e=Svqpyl

Introduction

Background to the problem:

The purpose of threat modeling, which is performed on the organization's application architecture and the technologies that will be utilized, helps us in the identification and mitigation of potential vulnerabilities in the application. Particularly for large and sophisticated applications, threat modeling can be challenging and needs to be performed consistently. Threat models need to be revised in corresponding with software systems updated and changed, which leads to keep the work in progress all the time. (Shostack, 2007) Manual and static methods are mainly used in the traditionally performed threat modeling, which might not be more helpful to keep updating with the continually changing threat scenarios. Threat models constructed sometimes cannot provide mitigations or protect against all possible cyber-attacks as they can only give accurate information accessible at the time of threat modelling. (Vijayan, 2018) Especially when the modelers are unaware of some potential vulnerabilities or attack methodologies which can be old or latest, threat modeling can sometimes fail in covering all possible threats or attack scenarios. This technological deficiency becomes worse by the threat actors' constant generation of new strategies, methods, and approaches to perform the attacks. Hence my implementing this model we are focusing on foreseeing the vulnerabilities effectively. (ThreatModeler, n.d.)
Threat feeds, incident reports, security studies, and dark web monitoring are some of the sources that gives information to threat intelligence. (Anon, n.d.) (Mate, 2022) These include all the latest attacks, vulnerabilities exploited, trends hackers developing, attack mechanisms. Cybersecurity specialists can gain profit from a more informed and flexible approach to threat assessment by indulging threat intelligence with threat modelling. Organizations can efficiently prioritize and manage resources, which are the most important threats/vulnerabilities while also maintaining an ideal defense posture, real-time and context-aware threat intelligence helps us in achieving our goal.

The technical challenge lies:

Forming a framework that is helpful in integrating the threat intelligence related information to threat modeling process or tools plays a critical role. Not having a licensed threat modelling tool which performs the threat modelling accurately leads to verifying multiple threat modelling tools and manual process. As the threat intelligence feeds give vast amount of data processing the data from different sources and verifying the accuracy

and reliability of the information creates a core phase in the research. Performing the data scrapping by using python scripting and manual ways is leading to ensuring the data format for utilizing I threat modelling as input. Interpreting and the proper relevance of the components in the architecture to the results from the threat intelligence and threat modelling helps to narrow our process and precise risks. Marking the severity of the vulnerabilities from the threat intelligence helps us to prioritize the threats and deviate from the general base line score. Eliminating the false positives and false negatives, analyzing real time threats, risk prevention and developing the mechanisms for the defense are some other technical aspects and challenges that play a key role.

Advantages/gaps this fill:

This integration helps organizations to stay updated and top of the emerging threats and threat patterns. This enables the potential understanding of the threats specific to components, applications, and process. Priority/ Severity of the threats will be changing which in turn helps to mitigate the potential vulnerabilities that are emerging and is crucial to business. This mechanism helps to develop the organization's defense systems against the threats emerging, real time insights on the targets and measures, remediations. Threat modeling, in combination with threat intelligence in the specific environment of the organization, ensures that the threat data is verified, which reduces the number of false positives, false negatives. The risk assessment would be more accurate and reliable overall since this validation procedure also enhances how well it can find real threats.

Use in industry:

Firms with sensitive data, organizations with digital infrastructures, sectors like financial institutions, healthcare organizations, government agencies, and large enterprises which are mostly targeted by hackers.

Objective of research:

- Performing the threat modelling to identify the potential threats.
- Verifying the real-world attacks and techniques to keep up to date and protect the organization.
- Assess the effectiveness of this integrated approach in identifying and prioritizing potential threats. Defining / updating the severity of the potential vulnerabilities
- Compare and contrast the results of traditional threat modelling and threat intelligence-infused threat modelling to demonstrate the advantages.

Plans to meet objectives:

To perform the integration and analysis the following steps can be followed:

1. **Creating Architecture Diagram:** To begin the analysis process we first create a architecture diagram of the application which includes the components and the flow of data. This helps to have the initial and crucial requirement for the analysis.
2. **Performing Threat Modelling:** Threat modelling will be performed on the prepared architecture diagram by using tool or manual process which is feasible based on architecture complexity and organizations financial budget. In this we have analyzed Microsoft threat modelling tool and also performed manual analysis. We will use OWASP ASVS security questionnaire checklist to understand the standard security requirements and CVSS scoring mechanism to rank the vulnerabilities.
3. **Threat intelligence data collection:** Thereat intelligence data can be collected from the various sources, such as security research, incident reports, and threat feeds, datasets published.
4. **Processing the Dataset:** Scrapping the threat intelligence dataset collected. We processed the data by using manual and python scripts. This dataset will provide insights into the latest threat patterns and trends. We also have CVSS scoring, component, threat details as main information.
5. **Relevance and integration of Threat Intelligence Reports**: Identify the threats reported from threat intelligence and map the issues with the components in the architecture diagram and threat modelling report. This helps to ensure the data is connected to identify the potential risks and attack vectors.
6. **Updating CVSS Scoring:** On merging the results we can update the severity of the potential vulnerabilities reported by using CVSS scoring system from the baseline rank given in threat modelling basing on the insights from the threat intelligence. This updated score helps in prioritizing the threats and understand the threat patterns to mitigate them.
7. **Updating remediation measures:** Based on the latest defense mechanism developed for the threats emerging and strong defense mechanisms should be suggested as remediation.

By following these steps, we can develop a mechanism for security strategy to secure the systems and applications from potential cyber threats rising.

Report structure:

The structure of the report includes multiple sections and subsections which starts with an abstract and ends with the conclusion. The abstract of the report consists of an overview of the idea behind the integration process and the glimpse of the results. On to the next section is introduction which talks about the basic topic that are being considered for the project and what are they this has threat modelling, threat intelligence and background of them. This also has the problem statement which in summary says that threat modelling process need to be updated with latest techniques. The technical challenges with the approach we will be taking up to overcome the problem. Advantages of the approach, framework we are taking up and moves to setting up the objectives to be chased. Plans to meet the objectives are also discussed in the Introduction phase. The second part of the report has a literature review which gives us knowledge about the trends around the objectives and then the overview of output to be expected and users of the output. The next part is about the methodology used in the framework and multiple activities that are performed to develop the framework. The framework here consists of OWASP threat modelling, OSINT, data scrapping that are discussed in the fourth part. This also includes tools utilized, programming languages used, vulnerability handling mechanism, overview of output, type of output, code written, data that is transformed, final stage implementation, results, and their details. The next is for the evaluation of the results, implications on the organizations. The next it is followed by results critical analysis. The final part includes explaining the efficiency of the framework, limitations that need to be considered, future development, commercialization of the process with the conclusion.

Literature Survey

According to the paper “Quantitative security assessment of power grid using Common Vulnerability Scoring System (CVSS) and attack traffic analysis” (Mate, 2022) describes a study on Cyber physical systems (CPS). These systems usually integrate components like network, computational, physical, and human components. CPS have a lot of importance in the current technologies as they are used in many industries like transportation, smart grids, power grids. Power grid systems are concentrated in this analysis. In this research to ensure the security of the cyber physical systems a security assessment framework using Common Vulnerability Scoring System (CVSS) is being evaluated. To perform this test research has done testing on physical devices like Smart Meter and performed attacks on them. Based on the attack severity CVSS scoring is derived and updated from the base line CVSS score allocated. SYN flood and Port Map attacks are performed on the Smart Meter and analyzed the change in severity which turns out to be increased. Based on attack scenarios considered, the CVSS score for two specific vulnerabilities, CVE-2021-22713 and CVE-2017-6048, were validated. As per the evaluation, Smart Meters having vulnerability CVE-2021-22713 were highly vulnerable to DoS attacks and less vulnerable to Port Map attacks, where in case of Smart Meters with the vulnerability CVE-2017-6048 have most likely same effects on DoS attacks and likely less impact on Port Map attacks. This shows the importance of updating the severity of the issues/ vulnerabilities based on the attack scenarios. Comparison of the different methods to rank the vulnerabilities is also done which is helpful to understand different methods available. In summary, this research presents quantitative strategy to improve power grid cybersecurity, this also helps cyber security teams to strengthen critical infrastructure based on real time threats.

As per the research paper “An Analysis of Various Cyber Threat Modeling” (Balamurugan, 2023) threat modelling is defined as a methodology used for identifying security controls and applying them into the design of software systems. Defining scope, identifying vulnerabilities, and developing countermeasures/remediations to reduce the consequences of cyber-attacks are all performed in the threat modelling approach, which aims to improve security across the network, processes, and devices. Using threat modelling to detect all potential threats in application, software engineers may include mitigations into their designs to prevent them and make them more reliable and safer. Threat modeling includes identifying a company's assets, defining the general utility of each program, and developing security profiles for each application. The next step involves identifying and ranking potential threats as well as tracking unforeseen threats and necessary remediation measures. The proposed research includes a information of many threat modeling techniques that are suitable for different environments, including "STRIDE, PASTA, OCTAVE, Attack trees, Security Cards, and CVSS."

STRIDE: STRIDE acronym for "Spoofing Identity, Tampering with Data, Repudiation Threats, Information Disclosure, Denial of Service, and Elevation of Privileges," defines six threat categories. This methodology aims to identify and mitigate potential risks before developing any line of code.
OCTAVE: “Operationally Critical Threat, Asset, and Vulnerability Evaluation" in short as OCTAVE. Two different methods were used to implement the OCTAVE technique: a) OCTAVE-S; and b) OCTAVE Allegro. OCTAVE-S is used in smaller organizations, to develop a protection strategy and mitigation strategies depending on the specific operational security risk of the organization. OCTAVE Allegro strategy is utilized, where it simplifies and optimizes the process of determining information security vulnerabilities, to gain accurate conclusions within a small amount of time, people, and other limited resources.
PASTA: A risk-focused threat-modeling system called PASTA which is acronym for Process for Attack Simulation and Threat Analysis. This includes important decision-makers, this methodology improves the threat-modeling process to a strategic level and requires security involvement from operations, governance, design, and development.
CVSS: CVSS stands for “The Common Vulnerability Scoring System” which identifies a vulnerability key trait and ranks their severity numerically, this is developed by NIST. CVSS is a standardized scoring system which users can access on multiple cyber and physical platforms and perform the scoring using the online CVSS calculator.
Attack trees: Attack trees helps to simulate the threats, this is the oldest and most used approach for "cyber-only systems, cyber-physical systems, and purely physical systems". This tree has root nodes, leaves, and child nodes which represent different assets, potential attacks, and targets.

According to the growing number of cyberattacks and to prevent them, cyber defenders must share cyber threat intelligence (CTI). This review of the literature in “Cyber threat intelligence sharing: Survey and research directions” (Wagner, 2019) researchers on the state-of-the-art and techniques many problematic areas with respect to the greater measure of exchanging cyber threat intelligence. The main aim of developing threat intelligence is to raise stakeholder awareness towards the vulnerabilities by informing them of the most recent threats and vulnerabilities and motivating them to act accordingly to address/remediate them.
As per the literature, stakeholders need to be a part of an effective and automated sharing process, but there aren't sufficient models and automated tools to make that possible and gives challenging environment. (Vázquez, 2012). Manually sharing of threat intelligence reports leads to consequences like slow sharing and new issues like human error while processing data, subjective relevance filtering. Based on law and regulations all the data cannot be shared in the same way or shared at all. Some data need to be anonymized which should also be considered. Sharing CTI with stakeholders who are not authorized or even present in the organization can cause risk. (Wagner, 2019). Likewise sharing CTI with competitor organizations encourages them to freely ride. If we didn’t share any information then it again leads to losing trust among stakeholders (Wagner, 2019).

Two protocols developed by US Government and Mitre are The Structured Threat Information Expression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII) are promising and well-liked protocols. These protocols take care of structural demands for cyber security such as evaluating cyber threats, defining indication of compromise, controlling reaction processes, and exchanging information on cyberthreats. CTI possesses several characteristics that processes it into true intelligence. CTI does not only includes malicious IP addresses or hashes on its own, but they may be a component along with others. Some attributes include descriptions of threat actors, campaigns, motivations, and indicators of compromise (IoC) shared with trusted stakeholders. Before considering CTI as actionable information concerning vulnerabilities must first be processed and submitted. Actionable CTI is defined by ENISA which meets five criteria: relevance, timeliness, accuracy, completeness, and ingestibility. (Schaberreiter, 2019)

The fundamental Threat intelligence platform (TIP) model had already been implemented, with the technique of mapping each data source individually. Each source has a unique broker class even if two sources provide csv formats with distinct column identifiers and format. The aim of this research “A Robust Architecture for Aggregation of Heterogeneous Data for Threat Intelligence Platforms” (A. Yasmeen, 2022) is to develop a way for targeted data models (TDMs) to format data in a single variant from a variety of sources, including Open Source Intelligence (OSINT), community sources, and internal sources. It should be able to apply TIP standards and map the source data appropriately for obtaining one format data. This work contributes by transforming data from disparate sources into a consistent format that might assist the TIP generate useful statistics. Different sources, each source considered can have different formats such as CSV, JSON, or TXT.

Data Collection layer, Data Mapping Layer, Data Aggregation, and modelling layer are part of the proposed methodology. Data from different sources is collected in the data collection layer and has different formats. Data mapping layer, in which the data from the data collection layer is inputted into XML broker which

has key value pair format. This layer contains a type of IoC, parameters assisting .XML file is utilized to optimize the whole system. In the last and final layer, the XML broker specifies where to map the feeds.
Main module of this architecture is the adapter which will map the input threat feeds into a targeted data model. Next comes the controller communicates with the internal model using xml service because it enables to perform changes clearly to the xml file. In the staging area aggregation will be performed and reflected to the target model. This directly influences the unified representation in this layer.

From the literature review on the multiple papers, we understood various technics that are being performed in the real world to perform multiple attacks. From the organization's perspective we understood how they are tackling the potential vulnerabilities and identifying them through threat modeling. Different methodologies, tools, and their limitations. Threat intelligence sources and data that is gathered plays a crucial role in understanding the threat patterns. Limitations on the threat modeling tasks that are being performed are explained clearly. This helps us to elaborate the advantages of the integration with threat intelligence.

Overview of output:
The results from the research help to understand the importance for organizations to keep updated about latest emerging cyber threats and they can be used in threat modelling process. Integrating threat intelligence into threat modelling gives organizations real time threat updates for specific systems, software's in an application, infrastructure level. This gives the latest threat patterns and helps us to develop proactive defense mechanisms. Organizations will have a clear understanding of their architecture and will be able to identify their assets and software. By interpreting the threat intelligence reports with threat modelling here we are focusing on prioritizing threats and remediating them also for having the more accurate and reliable risk assessment reports.

Potential users of output:
In all the ways performing this mechanism to find and remediate the potential vulnerabilities and keep updated on the latest trends helps organizations in several ways. All the stakeholders in the organizations would require the threat modelling report. This report is helpful in making decisions and prioritizing the action items for the security of the applications.
All the information security teams, security analysts would require having the information to monitor and perform vulnerability management, understand potential vulnerabilities. Available resources like systems, human source, tasking can be allocated basing on the vulnerability priority. Organizations can be updated with potential vulnerabilities and will be in a state of dealing with them. This helps to remediate/ take controls in the initial phase of development which in turn reduces the cost of remediation and loss due to cyber-attacks. During the audit or any cyber-attacks we will have an proper architecture of the application and the components used in the application, this makes it easy to understand the structure of the application and threat areas to focus on. Threat intelligence gives the indicator of compromise for the recent threats which makes it easy to perform the security checks on the infrastructure.

Research Methodology

Activities for project:
Performing literature review on latest threat modelling, threat intelligence research. Finding appropriate research papers, articles and doing a study on latest trends, finding best practices. Developing new data flow from the information. From the research conducted it leads to constructing architecture of small-scale domain hosting company. This required reviewing multiple infrastructure and software components. Analysis on different hardware and software components and infrastructure utilities for understanding of the different components and work areas. Analysis on how the data flow should be secured and what software components should be used to process the data.

Evaluating the Microsoft threat modelling tool and testing on application architecture to understand the working and limitations. This helps to have an understanding on how the tools work and different kinds of threats that they are generating. This also helps to understand updated versions of the tools and how feasible it is to use them. There are some drawbacks like the availability of infrastructure or software components to depict in the diagram and huge number of false positives. Since these are automated tools, the components depicted in the diagram are only consider that is the vulnerabilities related to the missing components are not generated in the risk assessment report. This has many advantages that can be considered for beginners but for developing a

complete architecture can be difficult due to limit compatibility, lack of advanced features. (Jeremy Geib, 2022) (Drake, n.d.)

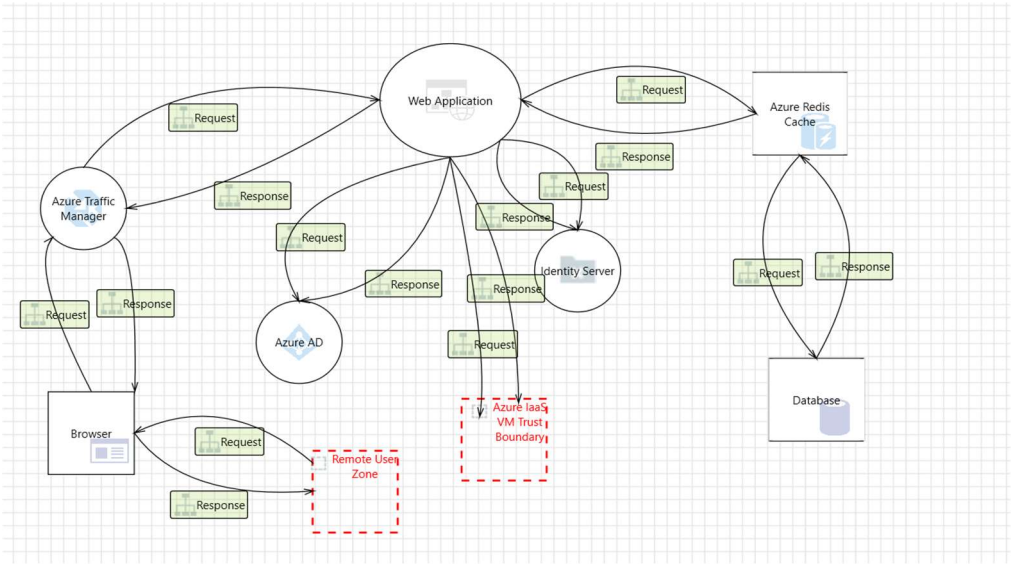


Fig 1: Architecture diagram from Microsoft Threat modelling tool

1. An adversary may guess the client id and secrets of registered applications and impersonate them [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	An adversary may guess the client id and secrets of registered applications and impersonate them
Justification:	<no mitigation provided>
Possible Mitigation(s):	Ensure that cryptographically strong client id, client secret are used in Identity Server. Refer: https://aka.ms/tmtcrypto#client-server
SDL Phase:	Implementation

2. An adversary may issue valid tokens if Identity server's signing keys are compromised [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	An adversary can abuse poorly managed signing keys of Identity Server. In case of key compromise, an adversary will be able to create valid auth tokens using the stolen keys and gain access to the resources protected by Identity server.
Justification:	<no mitigation provided>
Possible Mitigation(s):	Ensure that signing keys are rolled over when using Identity Server. Refer: https://aka.ms/tmtcrypto#rolled-server
SDL Phase:	Design

3. An adversary can get access to a user's session due to improper logout from Identity Server [State: Not Started] [Priority: High]

Category:	Spoofing
Description:	An adversary can get access to a user's session due to improper logout from Identity Server
Justification:	<no mitigation provided>
Possible Mitigation(s):	Implement proper logout when using Identity Server. Refer: https://aka.ms/tmtsmgmt#proper-logout
SDL Phase:	Implementation

Fig 2: Sample issues reported from Microsoft Threat modelling tools

In internet we can find different checklists to verify for the security of the applications among them we have taken OWASP standard questions version 4.0 (Govindraj Basatwar, 2022) as it has many areas covered and it has vast set of questions. Extracting the security questionnaire from the OWASP ASVS standard questionnaire which helps to understand the required security measures. (OWASP, 2019)

Going through and understanding different threat modelling methodologies like OWASP threat modelling, STRIDE, DREAD methodologies. Preparing a Threat modelling report structure, formulas for risk ranking from the methods explored, in this approach I have used CVSS scoring mechanism and STRIDE for threat categorization. (Conklin, n.d.) (Gonzalez, 2022) (T, 2022)

Calculation of Risk for the vulnerability can be performed basing on the formula: (Cipollone, n.d.)

*Risk = Probability (Likelihood of exploitation, Locality) * Severity * Impact*

Probability: Likelihood of the exploit by attacker
Locality: Defines the area which the vulnerability is limited to.

Severity: Consequences or effect of vulnerability

CVSS scoring for different severity: (CVSS, n.d.)

CVSS V3 SCORE RANGE	SEVERITY IN ADVISORY
9.0 - 10.0	Critical
7.0 - 8.9	High
4.0 - 6.9	Medium
0.1 - 3.9	Low

Table 1 : Severity from CVSS score

CVSS v3.1 scoring formulas that are standardized for calculating the risk score: (CVSS, n.d.)

The Base Score is a function of the Impact and Exploitability sub score equations. Where the Base score is defined as,

If (Impact sub score <= 0) *0 else,*

Scope Unchanged[4] $Roundup(Minimum[(Impact + Exploitability), 10])$

Scope Changed $Roundup(Minimum[1.08 \times (Impact + Exploitability), 10])$

and the Impact sub score (ISC) is defined as,

Scope Unchanged $6.42 \times ISC_{Base}$

Scope Changed $7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$

Where,

$ISC_{Base} = 1 - [(1 - Impact_{Conf}) \times (1 - Impact_{Integ}) \times (1 - Impact_{Avail})]$

And the Exploitability sub score is,

$8.22 \times AttackVector \times AttackComplexity \times PrivilegeRequired \times UserInteraction$

Temporal

The Temporal score is defined as,

$Roundup(BaseScore \times ExploitCodeMaturity \times RemediationLevel \times ReportConfidence)$

Environmental

The environmental score is defined as,

If (Modified Impact Sub score <= 0) 0 else,

If Modified Scope is Unchanged Round up(Round up (Minimum [(M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

If Modified Scope is Changed Round up(Round up (Minimum [1.08 × (M.Impact + M.Exploitability) ,10]) × Exploit Code Maturity × Remediation Level × Report Confidence)

And the modified Impact sub score is defined as,

If Modified Scope is Unchanged $6.42 \times [ISC_{Modified}]$

If Modified Scope is Changed $7.52 \times [ISC_{Modified} - 0.029]$-$3.25 \times [ISC_{Modified} \times 0.9731 - 0.02]$ 13

Where,

$ISC_{Modified} = Minimum$ [$[1 - (1 - M.IConf \times CR) \times (1 - M.IInteg \times IR) \times (1 - M.IAvail \times AR)]$, 0.915]

The Modified Exploitability sub score is,

$8.22 \times M.AttackVector \times M.AttackComplexity \times M.PrivilegeRequired \times M.UserInteraction$

4 Where "Round up" is defined as the smallest number, specified to one decimal place, that is equal to or higher than its input. For example, Round up (4.02) is 4.1; and Round up (4.00) is 4.0.

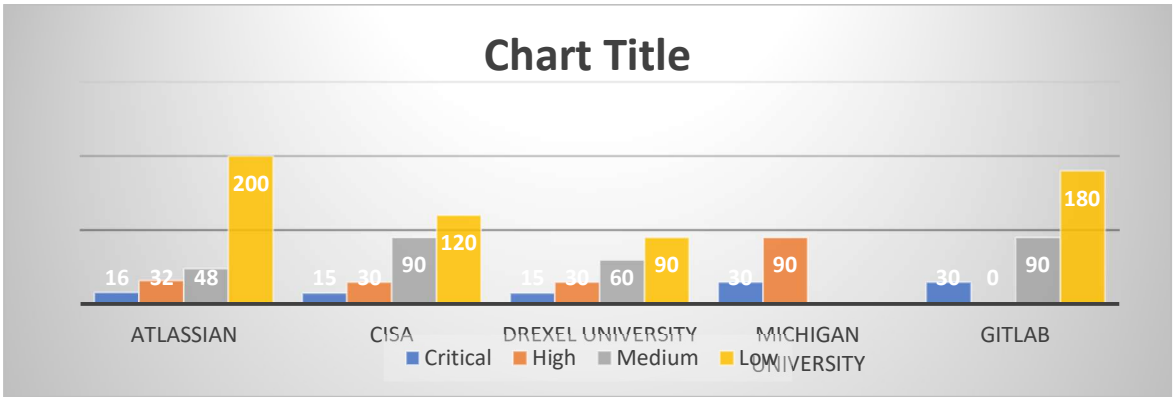
Formulas 1: CVSS scoring formulas

Remediation timeframes (SLA):

Different organizations will have different Service level agreements for the remediation of issues, considering some standard SLA's here from multiple organizations and standards we tried to find the minimum SLA that can be defined to remediate the issues. (Atlassian, n.d.) (Fortifydata, 2022) (university, n.d.) (michigan, 2022)

Company	Critical	High	Medium	Low
Atlassian	16	32	48	200
CISA	15	30	90	120
Drexel University	15	30	60	90
Michigan university	30	90		
GitLab	30	0	90	180

Table 2 : SLA's of different organizations/standards



Graph 1 : Graphical representation of SLA's

Exploring for the latest threat information in all the available open-source information available. The sources include threat feeds, threat intel reports, databases. Finding the threat reports and verifying the accuracy of the information, also looking if they are given a Common Weakness Enumeration (CWE) score or Common Vulnerabilities and Exposures (CVE) score. This ensures the validation of data and reliability of data.

Processing data from open-source reports which are in different formats and align them to a single format is the technical hurdle faced by all the industries. For this there are no developed tools which can help us to easy the process. There are frameworks which support to some extent, among them the framework used XML broker to process the data is discussed in the literature review. Have researched on python modules for data scrapping and used pandas module to format the data. (Daivi, 2023) (Gangwar, 2022)
Performed data scrapping manually and using python scripting on the threat intelligence dataset prepared.

Pandas: Used for data manipulation and analysis of the datasets.
Beautiful soup: Helps in parsing HTML and XML documents.
Scrapy: Can be utilized in generating pipelines in a structured way for scrapping web data.

Researching on the latest threats, attacks and updating the threat intelligence report with latest threats. The dataset selected is having the attacks from 2001 to 2020, hence updated the dataset with attack in latest years this ensures the dataset is up to the latest.

Different risk ranking mechanisms like DREAD, CVSS ranking on the threats are available for the threat modelling. On verifying the feasibility of the threat metrics CVSS scoring in appropriate for this project hence selected it. Here we have selected it as it is standardized ranking, and impact shown on different values. Risk assessment is performed for the threats reported. (Anon., n.d.)

Different attack mechanisms require different remediation measures hence explored the remediation mechanisms required for the attacks defines in the risk assessment report. Performing tests to eliminate false positives by verifying the security controls already implemented.

How the project is performed:

1. **Exploring the software, infrastructure for the small-scale information technology company. Creating an architecture diagram:**

The proposed architecture diagram is depicting a small-scale domain hosting service provider. This organization provides domains to the customers and for payment they are using a 3rd party payment service like bank via a payment gateway. This organization has different servers like DNS Server, LDAP, Windows server, virtual machines, database server, application server which perform different activities. Domain name conversion using DNS server, authentication and authorization services using LDAP, Windows server for file transfer, database server for transaction data processing, storing data, updating and application server for session management, connecting databases and services provided. Also, application gateway for URL based routing, health monitoring, SSL termination and virtual network gateway are used to connect on prem machines and virtual machines, data traffic is sent from the gateway.

The data flows from the user interface to web server passing via firewall to verify any threats. The internal firewall is connected to SIEM tool for threat identification. And a switch is used to connect with Wi Fi, printer, LAN connection.

The architecture is prepared using draw.io tool by analysing different components available.

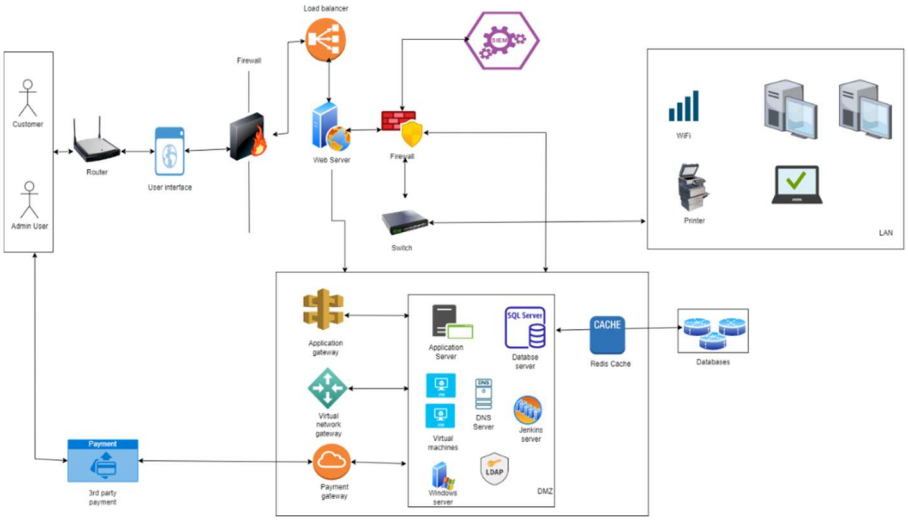


Fig 3 : Architecture diagram

Asset Inventory which explains all the software and hardware components that are present in the organization structure can be prepared and explain the basic purpose of the components. The following are the list of components:

- Customer and Admin Login panel
- Router, Switch
- Firewall, Internal Firewall
- Load Balancer
- Web Server, Application server, Database server, Jenkins server, DNS server, Windows server
- Virtual Machines
- LDAP
- SIEM tool
- Databases
- Payment gateway, Application Gateway, Virtual network gateway
- Printer, Wi Fi, PC's

2. **Answering the standard questions from OWASP ASVS**: (OWASP, 2019)

Based on the organization's architecture, assets and security controls identified we would answer the standard questions from OWASP as shown in Fig 4, these questions are given in "Security assessment quest" tab of OWASP ASVS document. This includes different topics like authentication, authorization, access management, database management, cryptographic controls, session management. This gives us the application risk score. We need to

answer the following questions basing on the architecture of the organization and implementation plan by giving the maturity value from 0 being lowest to 5 being most secure. Different maturity levels are given as explained in Fig 5 below to answer the questions. Once the questions were answered the results were generated basing on formula as shown:

For level 5:

Current maturity levels: =COUNTIFS('Security questionnaire'!$J$6:$J$376,B$7)

Target maturity levels: =COUNTIFS('Security questionnaire'!$K$6:$K$376,E$7)

For level 4:

Current maturity levels: =COUNTIFS('Security questionnaire'!$J$6:$J$376,B$8)

Target maturity levels: =COUNTIFS('Security questionnaire'!$K$6:$K$376,E$8)

Similarly for the other levels 3,2,1,0.

We can ignore the question by selecting the "No" in the "Selected" column, then these questions will not be considered for the risk calculation. All the Maturity levels used to answer the questions are considered to give the risk of application.

These questions are also analysed manually to understand the assets and controls in place. Vulnerability, weakness can be drawn from these questions and remediations can be provided. In our risk assessment report prepared in later stages we are going to write about vulnerabilities identified from these questions.

Section		Control	L1	L2	L3	Selected	Maturity Current	Maturity Target	Resid. risk	Co
V1: Architecture, Design and Threat Modeling Requirements										
V1.1 Secure Software Development Lifecycle Requirements										
V1	1.1.1	Verify the use of a secure software development lifecycle that addresses security in all stages of development.		x	x	Yes	2	4	2	
V1	1.1.2	threats, plan for countermeasures, facilitate appropriate risk responses, and guide security testing.		x	x	Yes	4	4	0	
V1	1.1.3	Verify that all user stories and features contain functional security constraints, such as "As a user, I should be able to view and edit my profile. I should not be able to view or edit anyone else's profile"		x	x	Yes	2	4	2	
V1	1.1.4	Verify documentation and justification of all the application's trust boundaries, components, and significant data flows.		x	x	Yes	4	4	0	
V1	1.1.5	Verify definition and security analysis of the application's high-level architecture and all connected remote services.		x	x	Yes	4	4	0	
V1	1.1.6	Verify implementation of centralized, simple (economy of design), vetted, secure, and reusable security controls to avoid duplicate, missing, ineffective, or insecure controls.		x	x	Yes	2	4	2	
V1	1.1.7	Verify availability of a secure coding checklist, security requirements, guideline, or policy to all developers and testers.		x	x	Yes	2	4	2	
V1.2 Authentication Architectural Requirements										
V1	1.2.1	Verify the use of unique or special low-privilege operating system accounts for all application components, services, and servers.		x	x	Yes	3	4	1	
V1	1.2.2	Verify that communications between application components, including APIs, middleware and data layers, are authenticated. Components should have the least necessary privileges		x	x	Yes	4	4	0	
V1	1.2.3	Verify that the application uses a single vetted authentication mechanism that is known to be secure, can be extended to include strong authentication, and has sufficient logging and monitoring to detect account abuse or breaches.		x	x	Yes	2	4	2	
V1	1.2.4	Verify that all authentication pathways and identity management APIs implement consistent authentication security control strength, such that there are no weaker alternatives per the risk of the application.		x	x	Yes	3	4	1	
V1.3 Session Management Architectural Requirements										

Fig 4 : Security assessment questionnaire

Level	Maturity	Description
0	Non-existing	Defined vulnerability is not considered as problem
1	Initial	While doing development this can be considered.
2	Defined	Implementation is developed but this depends on individual performance.
3	Standardised	Standard is developed and planned for implementation.
4	Verified	Implementation is developed and controls are tested.
5	Automated	Reached recommended controls by verifying the development constantly and automation.

Fig 5: Maturity levels definitions

3. Preparing the risk assessment report:

Analysing the OWASP ASVS questionnaire and architecture diagram we will find out the potential vulnerabilities and report them in the document. It includes details like the risk ranking of vulnerability using CVSS scoring, component/vulnerability, OWASP category, description of vulnerability, remediation measures to fix, source which says if the vulnerability is from architecture or OWASP ASVS questionnaire.

Issues identified from the architecture and security assessment questionnaire are Security Misconfiguration, Input validation, Identification and Authentication failure, Insecure design, Injection, Server-side request forgery. These are documented in the "TM" tab of "OWASP ASVS" excel document submitted. This document also includes other tabs like "threat categories" which shows the list of threat categories that can be considered to classify threat identified. "OWASP ASVS Original" tab which shows the set of questions downloaded from OWASP checklist.

The threats identified are carefully examined to relate with application, the threats are identified in manual review of architecture and questionnaire answered. Remediation measures were added to meet industry standards and risk ranking is performed using CVSS score calculator. Remediation timelines as explained in "Table 2 : SLA's of different organizations/standards" are verified to use them in our process.

S.No	Source (Architecture/questionnaire)	Threat category	Component	Description	CVSS score								Remediation	Remediation Timeline
					AV	AC	PR	UI	S	C	I	A	CVSS Base Score		
1	Architecture	Security Logging and Monitoring Failures	Log server	Logging and monitoring is ot performed, which shows that complaince requirements are not meet. Also there is no log management in case of log verification during an attack.	A	L	N	N	C	N	L	N	4.7	Place a logging and onitoring mechanism for user activity.	70
2	Questionnaire (v5.3 Output encoding and injection prevention requirements)	Identification and Authentication Failures	User interface Login functic	Passwords are generated in such a way that letters, numbers, few special characters are allowed. Output encoding, input verification is developed basing on this. This is prone to brute force attack and password policy no satisfied.	L	H	H	N	U	H	N	H	5.7	Update the password policy and implement the encoding mechanism	70
3	Questionnaire (v2.6 Lookup secret verifier requirements)	Insecure Design	Lookup secrets	Backup mechanism for 2FA failure is not implemented	A	H	H	R	U	N	N	H	4	Lookup secrets are used in case of failure in 2FA mechanism. Sever generated secret key is shared with client to utilize when the 2FA is not working.	70
4	Questionnaire(v5.2.7 Sanitizationa nd Sandboxing requirements)	Injection	Input sanitization	Application is not being santized for verify user supplied images, SVG files. This leads to different attacks like XSS, HTML attack, DoS, XML entity processing.	N	H	H	N	C	N	H	H	7.7	Prevent scripting tags, foreignobject, external links hould not be permitted inside the SVG image.	21
5	Questionnaire (v12.1 File Upload Requirements)	Server-Side Request Forgery	File Upload Functionality	File that are being upload not verified for size, zip files not being verified	L	H	H	N	C	N	H	H	7.2	Input file validation functionality like verifying file size, verifying file for any malicious data.	21
6	Architecture	Security Misconfiguration	Windows server	File transfer protocol controls firewall rules can be improved, other tan default site configuration, SFTP setup, certificate creation, virtual direotories configuration.	N	L	N	N	U	N	N	L	6.5	IIS (Internet Information Services) FTP (File Transfer Protocol) should have both active and passive modes enabled. In this client and server acts vice versa. Windows firewall should be configured with three rules FTP Server, FTP Server passive, FTP Server Secure.	70
7	Questionnaire (v2.1.4 Authentication verification requirements)	Input validation	Password validation	Unicode characters are not allowed										unicode chracters in password include symbols, special characters, characters from other languages which makes password more challenging to guess	
8	General practise		Scanning application	Perform SAST, DAST, SCA scans										Perform scanning while doing the development and set up automation pipelines for scanning.	

Fig 6 : Risk assessment report

4. **Threat intelligence:** (Valeriano, 2022)

Threat intelligence requires gathering of information about vulnerabilities, attacks, threat trends from open-source internet. For this project I have taken a dataset from the open-source internet which consists of different attacks and information related to the attacks. This dataset has cyber-attack related information from year 2001 to 2020 this consists of some important information like attack happened from, threat actors, affected people, source of attack, risk score, source details are given in the dataset.

Cyberincidentnum	Dyadpair	StateA	StateB	Name	interactionstartd	interactionend	method	severity	Political Objective	Sources1	Sources2
1	2365	US	Russia	Regin malv	02-01-2008	03-01-2011	3	4	Publically available sources claim that Reign malware sophisticated NSA backdoor, known to have infected Russian government networks and steal sensitive information	https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/regin-top-tier-espionage-tool-15-en.pdf	https://www.zdnet.com/article/infamous-regin-malware-linked-to-spy-tools-used-by-nsa-five-eyes-intelligence/
2	2365	US	Russia	QWERTY k	02-01-2008	03-11-2011	4.4	4	Publically available sources claim that Part of the Reign campaign, this sophisticated keystroke program was able to steal passwords and access secure networks	https://www.csoonline.com/article/2875739/microsoft-subnet/researchers-link-qwerty-keylogger-code-to-nsa-and-five-eyes-regin-espionage-malware.html	https://www.zdnet.com/article/infamous-regin-malware-linked-to-spy-tools-used-by-nsa-five-eyes-intelligence/
3	2365	US	Russia	Duke Serie	04-08-2008	9/17/2015	4.2	4	Access networks of geopolitical interest to Russia	https://www.f-secure.com/documents/996508/1030745/dukes_whitepaper.pdf	
4	2365	US	Russia	US govt en	08-06-2008	08-12-2008	4.2	3	To distract US diplomats in Tiblisi during the Five Day Russo-Georgian War of 2008.	http://www.ismlab.usf.edu/isec/files/Georgia-Cyber-Attack-NATO-Aug-2008.pdf	https://www.wired.com/2008/08/georgia-under-o/

Fig 7: Open-source dataset

5. **Updating the threat intelligence report information.**

The dataset selected is having attack details from year 2001 to 2020 year, hence updated the dataset with latest threat and attack details manually from the open-source internet. The latest attacks, threats added are Chat GPT Redis Cluster, D-Link, FortiOS, MOVEit. These are gathered from internet and is analysed to find the

relevance and truthfulness. On analysing these are processed to meet the format to add in the threat intel report. This dataset is uploaded in the artifacts with name “dataset.csv”

MOVEit: Windows server having vulnerable version of MOVEit file server. Unauthorized users can perform SQL queries on the databases. This attack leads to privileged escalation and gives unauthorized access to target environment. (Laboratory, 2023)

ChatGPT Redis Cache: radis-py which is open-source library caused a caching issue. This vulnerability has compromised sensitive users’ data like email address, name and credit card information. (Calrk, 2023)(OpenAI, 2023)

D-Link: In D-Link, D-view product with TftpReceiveFile Handler class this vulnerability exists. This allows an unauthorized attacker to execute arbitrary code. This vulnerability occurs due to improper validation of supplied path. (zerodayinitiative, 2023) (DLink, 2023)

FortiOS: Attacker can read and write any files in Linux system by crafting CLI commands. (Wikipedia, n.d.) (Dimitrova, 2023)

S.No	Dyadpair	StateA	StateB	Name	Component/Category	Description	Remediation	startdate	interactionenddate	CVSS score
1				Sensitive inforamtion disclosure	chat GPT Redis cluster	radis-py which is open source library caused a caching issue. This vulnerability have compromised senstive users data like email address, name and credit card information.	Redundant check were performed to ensure data accuracy. Improved logging. Developed patch for the vulnerability.	20-03-2023		3.7
2				SQL injection	Windows Server	Windows server having vulnerable version of MOVEit file server. Unauthorized users can perform SQL queries on the databases. This attack leads to privileged escalation and gives unauthorized access to target environment.	Disable all HTTP and HTTPS traffic to MOVEit environment. Verify and review al the access and delete unauthorized access. Update the patch provided. Update all the service account credentials. Enable the traffic to MOVEit.	15-06-2023		9.8
3				Arbitary code execution	D-link	In D-Link, D-view product with TftpReceiveFile Handler class this vulnerability exists. This allows an unauthorized attacker to execute arbitary	Update to the latest version released v2.0.1.28	28-12-2022		9.8
4				Path traversal	FortiOS	Attacker can read and write any files in linux system by crafting CLI commands	Update to latest version 6.4.12	07-03-2023		7.1

Fig 8 : Latest dataset

6. Performing the data scrapping on threat intel report.

To extract the required information for the analysis I have performed a manual and scripting using python for data scrapping. We will perform the scrapping of data to satisfy the format required in next phases while merging with threat modelling, we will keep only columns that are required as per the risk assessment report in threat modelling, this gives us same pattern. I have used Jupiter notebook to write the code and used pandas modules to process the data. The code is written in such a way that dataset processed in stored to a local machine by itself. With this step, we have completed the threat intelligence and acquired the latest threat information. We will be using this information now in threat modelling to update the risk assessment report. This helps to keep the threat modelling process updated with latest threats.

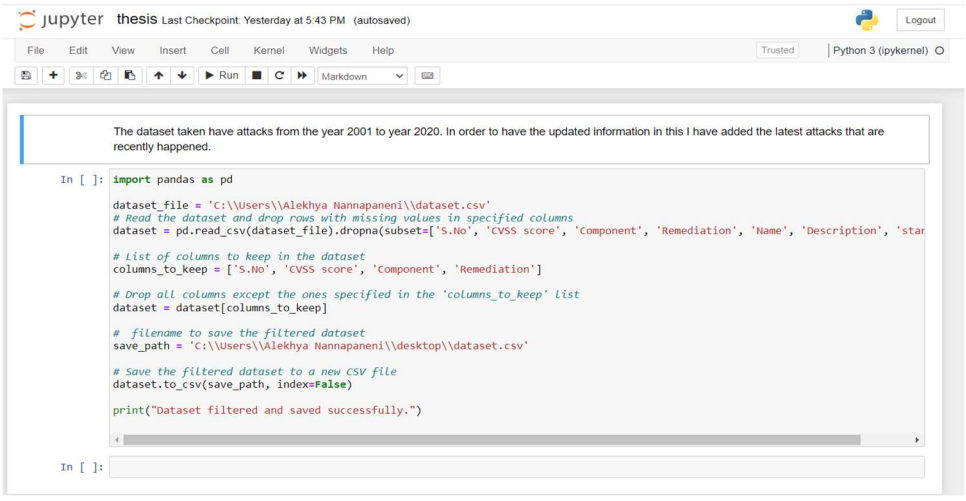


Fig 9 : Python script

7. **Align the threat intelligence report with risk assessment report.**

As of now we have prepared a risk assessment report by performing the threat modelling and latest threat information by using threat intelligence. Here to indulge the reports we will take data from both the reports and align them. This requires the mapping of architecture components like infrastructure or assets or software to threat intelligence report to know if there are any threats affecting the application directly. We need to find any patterns, functionalities, assets being affected and derive the threat patterns and how they are going to affect. Threats added would be given a new threat landscape relating to application, severity change, remediation timelines change. On being able to align the component we will update the risk ranking which can increase or deprecate basing on controls available, description, remediation measures which change following the latest defence technics. Also, if the threat noticed from threat intelligence is not present in the risk assessment report but affecting the application then a new threat be added to risk assessment report. Thus, indulging TM and TI reports adds new vulnerabilities and updates the existing vulnerabilities. This gives us the final/updated risk assessment report. The risk assessment report can be distributed among the stakeholders, cyber security teams, development teams for remediations and decision making.

Design and Implementation Specifications

Workflow followed:

The framework developed would be based on 4 different phases, mainly each being followed by multiple subtasks. They are Architecture, Threat Modelling (TM), threat Intelligence (TI), TM+TI.

Architecture:

This is the initial phase of the assessment. This involves performing the asset review where research for the software and hardware components required for the application. Then followed by the updating or preparation of asset inventory this is used to document all the components that are being used and the functionalities of the components. The main task is creating an architecture diagram, the application structure is developed and will be used in further assessment.

Architecure	Threat Modelling	Threat Intelligence	TM+TI
Component Analysis Asset Inventory Architecure diagram	OWASP ASVS Security questionnaire Threat identification Attack trees Risk assessment report Threat categorization Threat prioritization Remediation measures Threat description	OSINT framework Dataset collection Dataset Updation Data scrapping CVSS Scoring Remediation measures Description	Risk assessment report Threat categorization Threat prioritization Remediation measures Threat description

Fig 11: Workflow

The Open Web Application Security Project (OWASP) TM process: (Conklin, n.d.)

The threat modelling process developed by OWASP, who is a non-profit organization helps in developing the security standards and guidelines for the web application developers and organizations is a manual approach. The process developed for threat modelling with the aim of giving a standard, traditional methodology. This involves multiple phases for generating the risk assessment report and risk ranking. This gives us information about multiple potential vulnerabilities, severity score, remediations, assets list, dependencies, entry points, countermeasures, mitigations.

Phases involved:

1. **Decomposing the application**

To conduct assessment of an application we need to understand about the application which leads to performing different activities like identifying assets, external dependencies, entry points, exit points, functionalities, identifying trust boundaries. This gives us a clear understanding of how the application works and the components involved in the process.

Identify assets: Application requires many components to be a working model and perform the specified functionalities. All the software and hardware components are considered as assets for the organization. Examples include user login details, databases.

External dependencies: This consists of assets from 3rd party applications, these are in control of organization but cannot be developed or modified by internal teams. Examples include 3rd party payments, libraries.

Entry points: The interactions where data can be inputted or interacted with can be considered as entry points. Examples include login page, HTTPS port.
Exit points: Exit points are considered where data flows from the internal entity to the external entity. Examples include data access points.
Functionalities: Functionalities define the data flow, working model, output requirements, data need to be stored, processed.
Identifying trust boundaries: We can define the trust boundaries of the application by differentiating the entry points and exit points. The data where it flows from exit points and interacts with entry points will create a boundary or vice versa.
Data flow diagrams: In order to depict the data flow and components involved data flow diagrams are helpful. We can prepare different models for numerous components. These provide the visual representation of the application data. This gives an idea of data flow from end to end and helps us identify threats.

2. **Define and risk ranking**

Identifying threats, preparing attack trees, threats categorization, giving severity for threats are all part of the second phase in threat modelling. Identifying threats will be performed based on the data flow diagrams prepared from phase 1 which leads to preparing attack trees to the identified threats. Attack trees have child node, root that helps to give the attack in a structured format. Once we have the threats, attack trees prepared now we are going to classify the threats defined from the process which is called threat categorization. Later the threats will be given severity based on the CVSS scoring mechanism. With this now we have threats, threat categories and severity.

3. **Explain countermeasures and mitigations**

Countermeasures include following and verifying policies and standards to nullify/remediate the threats.
Mitigations are given for threats which require the issue to be fixed based on technical details and should be remediated. The threats identified will be given appropriate mitigations and followed for remediation.

Open-Source Intelligence (OSINT) Framework: (Gill, 2023)
This framework involves the collection of information or gathering of data from the open sources available like articles, databases, magazines, blogs, open internet sources, media, public government websites, research papers.
By using this framework information can be collected and processed to the required format. There are also many challenges that need to be considered while using this framework, for instance checking the relevance of the data, truthfulness of the data, updating the information to reflect the latest changes.
Relevance: The information we are looking at should be relevant to the field we are working in and needs to be linked to the infrastructure.
Truthfulness: Millions of data that would be generated in the internet every minute, they might have false information also circulating around. We need to verify the appropriate website and authorized websites to access the information.
Updated information: While working with the new technology we need to keep up with the latest information and techniques available. We need to observe the trends in the data and process the data accordingly.

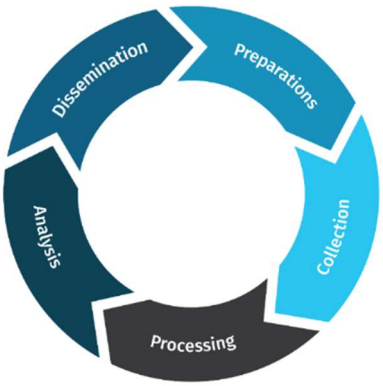


Fig 12: OSINT stages

Handling potential vulnerability:

The process of identifying the potential vulnerabilities, threat intelligence report and updating the risk assessment report will be an ongoing process as the trends for different attacks and techniques keep on

changing every time. It is advised to follow a process according to the developing needs. The below workflow diagram shows how a threats/vulnerability/attack trend detected need to be verified.

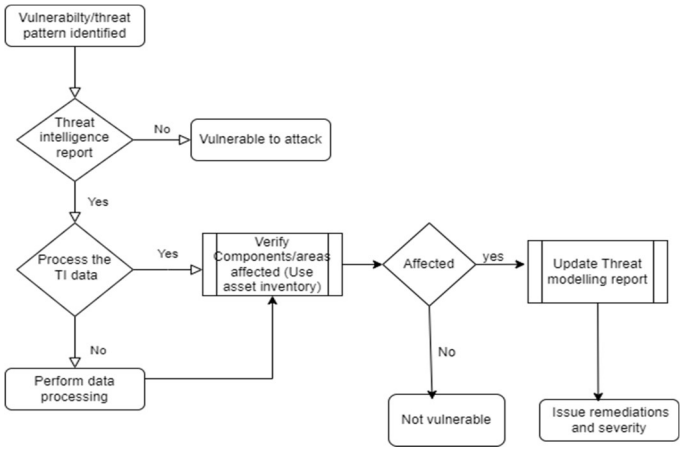


Fig 13: Vulnerability handling process

Final stage Implementation (TM+TI):

On performing the multiple tasks in threat modelling and threat intelligence we will have a risk assessment report and threat intelligence report. During the final stage of implementation, we will be using both the reports to indulge for the final step. Risk assessment report identifies the potential vulnerability in the application, explains it and provides complete details on how to apply countermeasures and mitigate the vulnerabilities. Threat intelligence reports provide real time threats, attacks and show the technical ways to provide countermeasures.

The drawback of having both the reports separately is that threat modelling works on known issues that might have lack of different attack scenarios to be considered or the reviewer might not have the knowledge of latest vulnerabilities. There is also a possible scenario that the reviewer could have made a mistake in validation. While conducting the threat modelling the attacks that are considered can be developed technically with new methodologies. In many organizations threat modelling performing risk assessment is not a continuous process which keeps updating on a timely basis. Due to this threat intelligence which keeps track of latest threat methodologies, trends should be considered in use along with threat modelling. Threat intelligence helps us in gaining insights of threats related to our environment. Data scrapping needs to be performed on the open-source reports to have the best utilization.

Here in the final stage of implementation we will be working to overcome the drawbacks on threat modelling by using the threat intelligence report we generated.

- Verify the components and assets in the architecture diagram and map the threat intelligence report with the architecture components and assets.
- On mapping we will understand which vulnerabilities, trends, attacks need to be considered from the threat intelligence report that are affecting the assets in the application.
- Now, verify the security issue and effects on the application. Once this is performed, we will be adjusting the severity, remediations according to the effect of the vulnerability on the application. Description explaining the new vulnerability and change of circumstances around it will be reported.

Output type:

The risk assessment report is the output produced from the research is in the format of excel. It includes details of the potential vulnerability, criticality score, remediation methods, information about vulnerability reported, component which is vulnerable.

Vulnerability type: Potential vulnerabilities that are identified from the analysis is given a threat category basing on standing OWASP Top 10 which can be Broken access control, Cryptographic failures, Injection, Insecure design, security misconfiguration, Vulnerable and outdated components, Identification and authentication failures, Software and data integrity failures, security logging ad monitoring failures, server-side request forgery.

CVSS score: CVSS scoring, which is used by many organizations as a standard risk rating, is used to rank the potential vulnerabilities identified. This includes different levels base score, temporal score, environmental score. We have used base score this this analysis this consists of ranking based on attack vector (AV). Attack complexity (AC), Privileges required (PR), User interaction (UI), scope (S), confidentiality (C), Integrity (I), availability (A). This CVSS score is reported from threat modeling with the base score and is updated based on the threat intel report summary. The severity can be increased based on attack mechanism, attack complexity in real world and can be reduced due to multiple mitigation controls in place.
Component: Component includes the attack name or the infrastructure, software name. This indicates the root place of the potential vulnerability.
Remediations: Different vulnerabilities have multiple types of remediations, these remediations are suggested to fix the possible vulnerability. These remediations are mostly suggested based on standards.
Description: A complete explanation of the vulnerability is given in the description. This includes how the vulnerability will affect, how are we saying this is vulnerability. In some cases, how the attack can take place, how the weakness can be leveraged.

Tools, languages used:

Jupyter notebook: (Anon., 2015) The Jupyter Notebook is an open-source, interactive web program that lets an user to write and share documents with live code, equations, illustrations, and explanatory notes. It's extensively utilized in fields like data analysis, machine learning, and scientific research. A notebook kernel is a computational engine which executes the code provided in a Notebook document. When we open a Notebook document, the associated kernel will be automatically launched. Notebook can be executed either cell-by-cell or all the cells, the kernel performs the computation and produces the results.
Microsoft threat modelling tool: This tool is designed for analyzing the security of the application that is developed by using the architecture diagram of the application. We can identify the potential security vulnerabilities and develop mitigations. This tool uses the STRIDE methodology for finding the threats and categorizing them. This gives the risk assessment report of the architecture.
Python programming language: Python is a high-level programming language, it's a free, open source and portable platform. Python has many functions and modules which make programming easy. Python programming language can be used in different fields like machine learning, web development, desktop applications. Python programs can be run on different platforms without any dependence.

Transformed data:

The details from the articles mentioned below is taken and processed to add in the threat intelligence dataset.
ChatGPT Redis Cache: Vulnerability leading to Sensitive Information disclosure is disclosed in ChatGPT, Asyncio redis-py client for Redis Cluster. The technical details and remediations are provided in the article from openai, theverge websites. The severity of the vulnerability is 3.7 low.
D-Link: zerodayinitiative, supportannouncement.us.dlink websites are taken as source to get the information related to this vulnerability. Remote code execution vulnerability raised in D Link, D View. Due to this vulnerability an unauthorized attacker can perform code execution. The severity of the vulnerability is given as 9.8 high.
FortiOS: FortiOS vulnerability is one of the highly targeted vulnerabilities in which a privileged attacker can read and write arbitrary files by using CLI commands. The source is sensorstechform website. The severity of the vulnerability is marked as 6.5 medium.
MOVEit: This vulnerability is related to file transfer in windows server. SQL queries can be performed on MOVEit databases. The severity of the vulnerability is 9.8 high.

Code written:

Python code written for data scrapping is using pandas module to structure the data. The code performs the data processing and prints the dataset to the local machines path defined in the code. The desired dataset file path is given to process. We should copy the file to the path where jupyter notebook is installed. The file is then read using pandas "pd.read". Once the file is inputted, we will start processing the dataset to print only required columns for the next phase. Here we are giving the column names "S.No, CVSS score, component, remediations" to print and delete the remaining columns which are not useful.

List of columns that need to be printed is defined.
Columns_to_keep=["S.No", "Component", "CVSS score", "Remediation"]

In order to save the file to the local machine in csv, path is defined, and csv format is being requested.
Dataset.to_csv=(save_path,index=false)

Potential Vulnerabilities identified as part of final implementation:
These findings are added in the "OWASP ASVS" document in tab "risk assessment report".

S.No	Source (Architecture/questionnaire)	Threat category	Component	Description	CVSS score								Remediation	Remediation Timeline
					AV	AC	PR	UI	S	C	I	A	CVSS Base Score		
7	Architecture	Security Misconfiguration	Windows server (MOVEit)	MOVEit used for file transfer is having a vulnerability that leads to unauthorized access to databases. File transfer protocol controls firewall rules can be improved, other tan default site configuration, SFTP setup, certificate creation, virtual directories configuration.	N	L	N	N	C	L	L	L	9.8	Disable http, https traffic and verify all the access. Update the patch at the earliest. IIS (Internet Information Services) FTP (File Transfer Protocol) should have both active and passive modes enabled. In this client and server acts vice versa. Windows firewall should be configured with three rules FTP Server, FTP Server passive, FTP Server Secure.	15
8	Architecture	Arbitary code execution	D-link	In D-Link, D-view product with TftpReceiveFile Handler class this vulnerability exists. This allows an unauthorized attacker to execute arbitary code. This vulnerability occurs due to improper validation of supplied path.	N	H	H	N	C	H	H	H	8	Update to the latest version released v2.0.1.28	15
9	Questionnaire (v2.1.4 Authentication verification requirements)	Input valdation	Password validation	Unicode characters are not allowed	A	H	H	N	U	L	L	L	3.9	unicode chracters in password include symbols, special characters, characters from other languages which makes password more challenging to guess	90

Fig 13: Risk assessment report

Finding 1:
Vulnerability detected is derived from the architecture diagram components that are mentioned. We can find a windows server and the functionalities of the server include file services, remote access services, communications. The best practices to keep the server secure is to have authorized access, access control mechanisms, disabling http traffic, having active and passive modes. From the OWASP ASVS questionnaire answered we were not able to clearly identify the security controls mentioned for the windows server hence we have reported a vulnerability security misconfiguration with the severity medium 6.5 and remediation timelines of 70 days to fix it. As per the real time threats a vulnerability identified in the MOVEit file transfer mechanism which is being used in windows server. This vulnerability leads to unauthorized access. Hence the severity of the vulnerability is raised to critical 9.8 and given service level agreement (SLA) remediation to fix in 15 days. The remediation advice provided by legal authorities is to disable all the traffic and verify unauthorized access. Update to the latest version possible to remediate the vulnerability.

Finding 2:
From the architecture diagram hardware components depicted we have a modem that is being used for the networking. Mostly all the modem and router configurations are managed by the internet providers and internal team members in the organization are responsible for the very few configurations required to block some traffic or impose any restrictions on IP addresses. Hence here we have not identified any vulnerability. Later on from the OSINT we identified a vulnerability that is discovered in the D Link D view component and is requires remediation measures to be taken to avoid from any attack. Hence this is included in the risk assessment report with severity high 8 score. The remediations include the verification of access and prevent any invalid inputs supplied in the path. This requires monitoring for any access issues and the permanent fix would be updating the security patch.

Finding 3:
The input validation detected shows the best practices for the validation of input and what type of inputs need to be accepted. This is not a vulnerability that is detected from the OWASP ASVS questions, it's only best practice and is marked as informational. Later on, from the attack trends we observed that the concern leading to input validation vulnerability is Unicode. Attackers are developing techniques to input Unicode in passwords and URL or any other entry points. Due to this informational suggestion input is updated to low 3.9 severity vulnerability with remediations saying that mechanisms need to be developed to detect Unicode characters and allow users to input Unicode characters in password to prevent from brute force attacks and also to verify for Unicode characters in the entry points.

Evaluation and Implications:

Evaluation:

There are certain evaluations we need to perform on the threat intelligence data that we were using to satisfy conditions like reliability, relevance, impact, alignment with the organization. (Bauer, 2020) Likewise for threat modelling process we can evaluate if it has effectiveness, mitigation strategies feasibility, timelines. (Shevchenko, 2018)

Reliability: The data that is being used should be tested to determine if we can rely on the information that is being provided. Since the data is collected by the open-source provider the attacks that are consider is revalidated again different sources available. They are official websites for the products/assets that we used in the application. The information collected in verified against the data provided in the open-source internet.
Relevance: The information that is being linked with the requirements only needs to be adopted. For instance, we used vulnerability related to D- Link because we have a D- link modem that is being used in the application. This is verified manually against the vulnerabilities gathered by linking with application.
Impact: It is important to see how impactful the methodology that is being adopted is helpful to achieve the target. This is identified by verifying the level of security against the vulnerabilities this method is providing. The remediations that are being provided in this are creating a more secure application.
Effectiveness: The main criteria that needs to be validated is the effectiveness of the implementation. There are cases where it is much more effective to use the methodology to obtain better results. In this case we have found it to be more effective to implement it as we are able to keep updated with the latest vulnerabilities.
Feasibility: The feasibility of the methodology can be verified by checking on the required resources to implement the methodology. This methodology can be implemented in small scale organizations as they have applications which can human process in specific timelines. In a large-scale organization with multiple applications and large applications it requires automation process to perform this methodology continuously.
Timelines: As the process is performed manually the timelines required are slightly higher than the normal process. This process can be automated to perform threat modelling and threat intelligence using tools. Then again python scripting can be written to process the reports. This requires less time than the manual process.

Implications:

This approach for performing threat modelling creates huge positive implications on the organizations. This changes the cyber security practices that organizations are following and keep them up to date.
Some of the implications are as follows:
Effective defense mechanism: Customization of defense mechanism can be performed according to attack trends that are being developed by attackers. Organizations can develop their own and feasible solutions to the vulnerabilities as they will be having enough timelines to take measures and discuss, research on different options and mechanisms that can be developed which will suit their application.
Update knowledge / continuous development: As we will be researching and keeping track of all the trends, attacks mechanisms that attackers are developing, we will have knowledge of all the latest attacks. This is on going process hence it will be a continuous development and knowledge seeking.
Enhanced risk identification: Risk assessments performed by considering only the in-build architecture and security related questions answered helps to an extend to find the vulnerabilities but finding the vulnerabilities using threat intelligence along with threat modelling adds an enhanced layer of security.
Accurate decision making: Stake holders can make decisions in a timely manner by considering the different aspects. Vulnerability prioritization gives them a clear understanding of required time and resources.
Cost saving: Fixing the vulnerabilities by predicting the occurrence and taking the countermeasures to minimize the risk before it hits our infrastructure or the application helps in saving cost as this helps us to prevent from security breaches, malware, unauthorize access, sensitive data protection.

Critical Analysis of Results and improvements:

Finding 1: Security Misconfiguration:

TM (Risk assessment report)	TM+TI (Risk assessment report)
Source: Windows server MOVEit CVSS: 6.5 Remediation: Update active and passive modes	Source: Windows server MOVEit CVSS: 9.8 Remediation: Update patch available. Verify unauthorized access

Table 3: Security misconfiguration

In the application architecture provided we observed windows server running which has a file transfer functionality with MOVEit. In the risk assessment report, we depicted the vulnerability to be medium issue with requirement of active and passive mode enabling requirement for the remediation of the issue.

Later, gathering the threat intelligence report we identified a security misconfiguration vulnerability which is being exploited. MOVEit File transfer application which is running in windows server is exposed to a vulnerability which can lead to unauthorized access and privilege escalation. This vulnerability allows an attacker to perform code SQL commands against the targeted databases. The attacker then further exploited this vulnerability to arbitrary file upload.

This information from the threat intelligence report shows the windows server is prone to attack. Hence we have updated the risk assessment report to reflect the latest attack and the remediations required.

Finding 2: Directory traversal remote code execution:

TM (Risk assessment report)	TM+TI (Risk assessment report)
Source: D link D view modem CVSS: N/A Remediations: N/A	Source: D link D view modem CVSS: 8 Remediations: Update to the latest version available.

Table 4: Directory traversal remote code execution

In the initial phase the D Link configurations are suggested to be verified to prevent the attacks on it. On analyzing the threat intelligence reports we have identified a vulnerability. D-Link modem used in the application turns out to be vulnerable to remote code execution due to TftpReceiveFileHandler class. This is raised due to improper validation of user supplied path and an unauthorized user can perform this attack.

Basing on the vulnerability identified to have updated the cvss scoring and the remediation measures for the D Link component. Thus, the threat intelligence report helped in securing the D Link modem.

Finding 3: Input validation:

TM (Risk assessment report)	TM+TI (Risk assessment report)

Source: User login CVSS: Informational Remediations: unicode characters in password include symbols, special characters, characters from other languages which makes password more challenging to guess.	Source: User login CVSS: 3.9 Remediations: Whitelisting of characters allowed in suggested in passwords. For the other entry points like URL's verifications need to be performed to check unicode characters

Table 5: Input validation

Using Unicode characters for the password in login functionality will be the best practice that security experts suggest. There are mechanisms being developed around the Unicode functionality in computing, but they are not being completely used in the login. Developers usually perform whitelisting of the allowed characters, and they don't include Unicode characters. This gives a chance for the brute forcing of passwords. Likewise in the URL's domain names can be easily morphed with change in some characters. Computers will consider this as a different character but, in the URL, they look similar with slight change.
On looking at the developing attacks and trends using the Unicode characters it is reported to take proper measures to avoid input validation errors. Hence it is given a CVSS of 3.9 and remediation measures were given as entry point verification and use of Unicode character in password while it is only informational and best practice earlier.

All the reports collected from the threat intel might not be considered as they cannot be relevant ot our application sometimes. For example, the vulnerability recorded in the dataset ChatGPT Redis Cache vulnerability using radis-py open-source library causing a caching issue. This is not recommended to use in the risk assessment report as it is not anywhere related to our application.

Modifications and improvements that can be developed to the design to enhance the results includes the following:

Threat hunting: The purpose of threat hunting is to perform continuous monitoring of traffic and identify any possible malicious activities which can lead to breach. Threat hunting should be continuous process and should have end point security. (vmware, n.d.)
Training: Employees should be trained to immerse themselves in the framework and should be educated about the process.
Metrics: Organizations can prepare the metrics and graphs to understand the effectiveness of the framework and developments that can be performed for improvement of the framework.
Automation: Libraries can be developed for the threat intelligence sources collection, certain features in the tools can be created to perform automation of threat findings, severity scoring.

Conclusions and Discussion/Future work

The objectives behind the research performed are stated to safeguard the application and infrastructure. The achievements of these goals determine the organization's focus on preventing cybersecurity attacks. The aim of developing an effective framework helps us achieve our target of identifying potential vulnerabilities that are emerging in the real world and techniques being developed by attackers. This helps the organizations to protect from unwanted cyber threats. OWASP threat modelling approach gives the base steps for preparing the risk assessment report which makes the process worthy, this makes the threats identification more effective. The results between the traditional threat model and combined approach for threat intelligence and threat modelling were comprehensively explained with the findings from the risk assessment report.

The efficiency of the indulging threat intelligence into threat modelling research performed offers several advantages, which includes:

- Relevance of the threats identified has increased, due to threat intel information. This leads to accuracy in finding threats.
- The effect of threat modelling in finding threats increased due to updated technics, attacks, vulnerability being added and severity, remediations are according to the threats.

- All the employees who are responsible for the security of applications, stakeholders, are notified and on track about the vulnerabilities around.
- Remediations and severity of the vulnerability are updated up to the level.

Limitations:

However, there are some limitations in the framework followed which makes the process slow and time consuming. There are even the chances of human errors.

- Manual processing of all the open-source information leads to managing many sources list and takes lot of time to process. The information needs to be converted to the required format.
- The process of performing the data cleansing can lead to errors sometimes like overlooking the minute details required, prioritizing the information without complete understanding, formatting the data leads to loss of data. There are chances of losing track of data.
- Threat modelling process manually performed requires an expertise reviewer, even though there can be cases where human error can occur.

Proposals for future work and potential for commercialization:

As there are no well-developed automation tasks for threat intelligence there is lot of scope in developing frameworks, technics for the information gathering and processing. The complete framework which is manually performed can be automated by using a commercial threat modelling tool, generating automation scripts for data scrapping. Python scripting can be developed to create libraries for threat intelligence and processing data.

All the organizations consider security of the applications as a priority aspect to avoid many consequences and to have the reputation of the company. This framework gives an opportunity to identify the threats before the development and make changes to the implementation which leads to cost saving and adds an extra layer of security to the applications. The process can be completely automated and commercialized.

Conclusion:

In conclusion, the integration of threat intelligence into threat modelling is a strategical approach as well as dynamical approach that enables the organizations to secure their applications, infrastructure. By following this approach organizations can feel the stability to prevent the real time vulnerabilities. Threat intelligence reports from the open-source internet provide lot of advantages in the organizational security for identifying threats scenarios, attack trends, remediation strategies as per the emerging threats. This encourages us to build a continuous assessment model for identifying potential threats. This involves the stakeholders and provides then insights into the vulnerabilities that can affect. Integration helps the organization to move forward in a secure manner.

References

A. Yasmeen, A. M. a. K. K. U., 2022. *A Robust Architecture for Aggregation of Heterogeneous Data for Threat Intelligence Platforms,.* Islamabad, Pakistan, 24th International Multitopic Conference (INMIC).

Adam, 2007. *trouble.* [Online]
Available at: https://www.microsoft.com/en-us/security/blog/2007/09/26/the-trouble-with-threat-
[Accessed 1 8 2023].

Anon., 2015. *1. What is the Jupyter Notebook?.* [Online]
Available at: https://jupyter-notebook-beginner-guide.readthedocs.io/en/latest/what_is_jupyter.html
[Accessed 1 8 2023].

Anon., n.d. *EC Council Cybersecurity exchange.* [Online]
Available at: https://www.eccouncil.org/cybersecurity-exchange/threat-intelligence/dread-threat-modeling-intro/
[Accessed 25 7 2023].

Anon, n.d. *Threat intelligence - definition & overview..* [Online]
Available at: https://www.sumologic.com/glossary/threat-intelligence/#:~:text=mitigate%20known%20threats.-,Threat%20intelligence%20can%20be%20derived%20from%20external%20sources%2C%20such%20as,SIEM)%20or%20log%20management%20tool
[Accessed 2 7 2023].

Atlassian, n.d. *Severity Levels for Security Issues.* [Online]
Available at: https://www.atlassian.com/trust/security/security-severity-levels
[Accessed 28 7 2023].

Balamurugan, K., 2023. *An Analysis of Various Cyber Threat Modeling..* s.l., IEEE.

Bauer, S. F. D. S. C. L. S. S. D. a. B. R., 2020. *Towards an Evaluation Framework for Threat Intelligence Sharing platforms.* s.l., s.n.

Calrk, M., 2023. *ChatGPT's history bug may have also exposed payment info, says OpenAI.* [Online]
Available at: https://www.theverge.com/2023/3/24/23655622/chatgpt-outage-payment-info-exposed-monday
[Accessed 6 8 2023].

Cipollone, F., n.d. *Vulnerability timelines, SLA, Measurement and prioritization – the how and the why of application and cloud security objective setting.* [Online]
Available at: https://phoenix.security/vulnerability-timelines-sla-measurement-and-prioritization-the-how-and-the-why-of-application-and-cloud-security-objective-setting/
[Accessed 25 7 2023].
community, P., 2023. *MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362).* [Online]
Available at: https://community.progress.com/s/article/MOVEit-Transfer-Critical-Vulnerability-31May2023
[Accessed 5 8 2023].
Conklin, L., n.d. *Threat Modeling Process.* [Online]
Available at: https://owasp.org/www-community/Threat_Modeling_Process
[Accessed 18 7 2023].
Conklin, L., n.d. *Threat Modeling Process.* [Online]
Available at: https://owasp.org/www-community/Threat_Modeling_Process
[Accessed 14 7 2023].
CVSS, n.d. *Common Vulnerability Scoring System version 3.1: Specification Document.* [Online]
Available at: https://www.first.org/cvss/specification-document
[Accessed 24 7 2023].
Daivi, 2023. *7 Python Libraries For Web Scraping To Master Data Extraction.* [Online]
Available at: https://www.projectpro.io/article/python-libraries-for-web-scraping/625
[Accessed 25 7 2023].
Dimitrova, M., 2023. *CVE-2022-41328 in FortiOS Exploited in Highly Targeted Attacks.* [Online]
Available at: https://sensorstechforum.com/cve-2022-41328-fortios/
[Accessed 7 8 2023].
DLink, 2023. *(Non-US) D-View 8 : v2.0.1.27 and below : TrendMicro (ZDI) Reported Multiple Vulnerabilities.* [Online]
Available at: https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10332
[Accessed 7 8 2023].
Drake, V., n.d. *Threat Modeling.* [Online]
Available at: https://owasp.org/www-community/Threat_Modeling#:~:text=Threat%20modeling%20is%20a%20family,of%2C%20threats%20to%20the%20system
[Accessed 20 7 2023].
Fortifydata, 2022. *FortifyData's Alignment with NIST SP 800-40.* [Online]
Available at: https://fortifydata.com/blog/fortifydata-alignment-with-nist-sp-800-40/
[Accessed 28 7 2023].
Gangwar, M., 2022. *Python Pandas Module Tutorial.* [Online]
Available at: https://www.digitalocean.com/community/tutorials/python-pandas-module-tutorial
[Accessed 25 7 2023].
Gill, R., 2023. *What is Open-Source Intelligence?.* [Online]
Available at: https://www.sans.org/blog/what-is-open-source-intelligence/
[Accessed 28 7 2023].
Gonzalez, C., 2022. *Top 8 Threat Modeling Methodologies and Techniques.* [Online]
Available at: https://www.exabeam.com/information-security/threat-modeling/
[Accessed 23 7 2023].
Govindraj Basatwar, G. B. H., 2022. *OWASP Application Security Verification Standard (ASVS).* [Online]
Available at: https://www.appsealing.com/owasp-asvs-application-security-verification-standard/
[Accessed 18 7 2023].
Jeremy Geib, B. S. D. C. k.-M. J. H. M. B. B. K., 2022. *Microsoft Threat Modeling Tool.* [Online]
Available at: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool
[Accessed 20 7 2023].
Laboratory, I. T., 2023. *NATIONAL VULNERABILITY DATABASE.* [Online]
Available at: https://nvd.nist.gov/vuln/detail/CVE-2023-34362
[Accessed 5 7 2023].
Mate, V., 2022. Quantitative security assessment of powergrid using Common Vulnerability Scoring.
michigan, U. o., 2022. *Vulnerability Remediation.* [Online]
Available at: https://safecomputing.umich.edu/protect-the-u/protect-your-unit/vulnerability-management/remediation
[Accessed 28 7 2023].
OpenAI, 2023. *March 20 ChatGPT outage: Here's what happened.* [Online]
Available at: https://openai.com/blog/march-20-chatgpt-outage#technical-details
[Accessed 5 8 2023].
OWASP, 2019. *Application Security Verification Standard 4.0.* [Online]
Available at: https://owasp.org/www-pdf-archive/OWASP_Application_Security_Verification_Standard_4.0-en.pdf
[Accessed 16 7 2023].
Schaberreiter, T. K. V. R. K. S. A. P. A. I. C. a. Q. G., 2019. *A quantitative evaluation of trust in the quality of cyber threat intelligence sources..* s.l., 4th international conference on availability, reliability and security .
Shevchenko, N. F. B. a. W. C., 2018. *Threat Modeling: Evaluation and Recommendations..* s.l., Carnegie Mellon Univ. Softw. Eng. Inst..
Shostack, A., 2007. *The Trouble with Threat Modeling.* [Online]
Available at: https://www.microsoft.com/en-us/security/blog/2007/09/26/the-trouble-with-threat-modeling/
[Accessed 1 7 2023].
ThreatModeler, n.d. *THE ULTIMATE GUIDE TO THREAT MODELING.* [Online]
Available at: https://threatmodeler.com/the-ultimate-guide-to-threat-modeling/
[Accessed 2 7 2023].

T, M., 2022. *What is STRIDE Threat Model?.* [Online]
Available at: https://www.practical-devsecops.com/what-is-stride-threat-model/
[Accessed 23 7 2023].
university, D., n.d. *VULNERABILITY MANAGEMENT.* [Online]
Available at: https://drexel.edu/it/security/services-processes/vulnerability-management/
[Accessed 28 7 2023].
Valeriano, B., 2022. *Dyadic Cyber Incident Dataset v 2.0.* [Online]
Available at: https://dataverse.harvard.edu/file.xhtml?fileId=6503190&version=1.0
[Accessed 1 7 2023].
Vázquez, D. A. O. S. C. B. S. a. R. E., 2012. *Conceptual framework for cyber defense information sharing within trust relationships..* In 2012 4th International Conference on Cyber Conflict (CYCON 2012) (pp. 1-17). IEEE., IEEE.
Vijayan, J., 2018. *7 threat modeling mistakes you're probably making.* [Online]
Available at: https://www.csoonline.com/article/564539/7-threat-modeling-mistakes-you-re-probably-making.html
[Accessed 1 7 2023].
vmware, n.d. *What is Threat Hunting?.* [Online]
Available at: https://www.vmware.com/in/topics/glossary/content/cyber-threat-hunting.html#:~:text=Threat%20Hunting%20is%20a%20security,find%20and%20stop%20malicious%20activities
[Accessed 1 8 2023].
Wagner, T. M. K. P. E. a. A. A., 2019. Cyber threat intelligence sharing: Survey and research directions. *Computers & Security,* Volume 87, p. p.101589..
Wikipedia, n.d. *Fortinet.* [Online]
Available at: https://en.wikipedia.org/wiki/Fortinet#:~:text=Fortinet%20is%20a%20cybersecurity%20company,Fortinet%2C%20Inc.
[Accessed 8 8 2023].
zerodayinitiative, 2023. *D-Link D-View Use of Hard-coded Cryptographic Key Authentication Bypass Vulnerability.* [Online]
Available at: https://www.zerodayinitiative.com/advisories/ZDI-23-714/
[Accessed 7 8 2023].