CHAPTER II
LITERATURE REVIEW

2.1 Theoretical basis

This writing approach basically explains important theories related to theories regarding grand theory, middle theory, and applied theory to support research. Grand theory, middle theory, and also applied theory are the unified basis used in preparing research.In this section, the theoretical basis will be explained which aims to provide a strong conceptual basis for preparing research. This research contains 3 theoretical foundations consisting of grand theory, middle theory and applied theory. Figure 2.1 shows an overview of the theoretical basis.

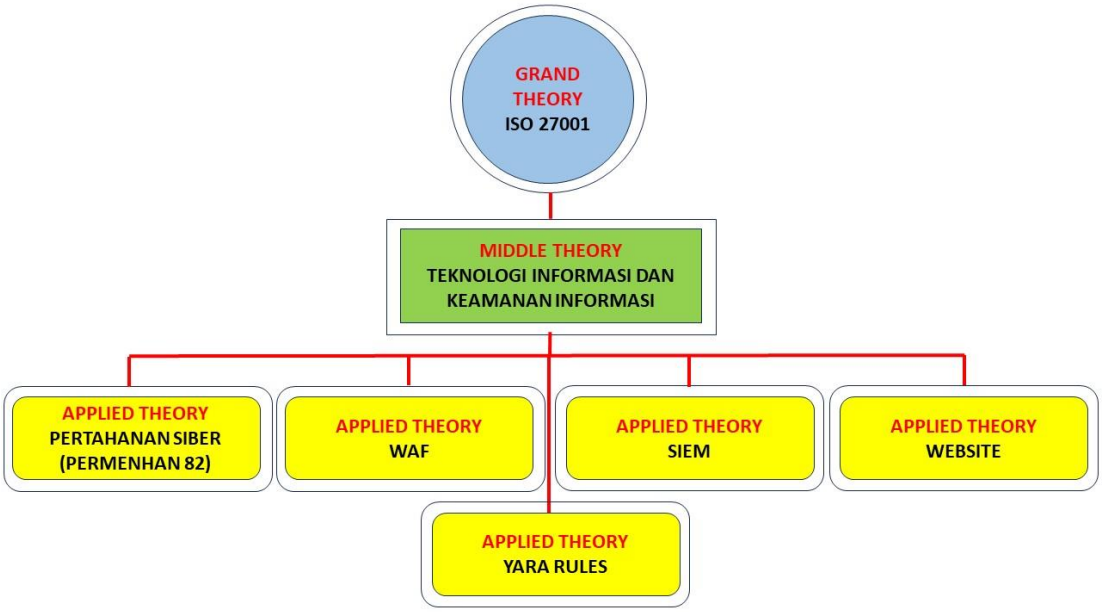

Figure 2.1 Theoretical basis
Source: Developed by the Author

Grand Theory is the basis for the birth of other theories at various levels. They are called macro because these theories are at the macro level (Dougherty & Pfaltzgraff 1990, 10-11). Grand Theory is a main concept used by researchers to allocate information about the hypothesis to be used. The purpose of this grand theory is to support research that is based on the results of research gaps and also certain scientific thinking frameworks. This grand

theory is abstract because it consists of the most important concepts used to understand the problems faced.

2.1.1 ISO 27001

Harris (2021, p.55) explains that ISO 27001 originates from British Standard 7799 (BS7799) which was developed by the British Department of Trade and Industry and published by the British Standards Institution in 1995 with the aim of providing guidance for organizations on how to design, implement, and maintain policies, processes, and technology to manage risks to its sensitive information assets. Harris (2021, p.55) states that the reason why this kind of standard is needed is so that security controls in an organization can be managed centrally and implemented throughout the organization. Without centralized security management, security controls will be implemented and managed separately and not optimally.

According to Harris (2021, p.209) ISO 27001 is a standard for establishing, implementing, controlling and developing an Information Security Management System (ISMS). Harris (2021, p.209) defines ISMS as a coherent set of process policies and systems for managing risks to information assets as outlined in ISO 27001. ISO 27001 includes requirements for assessing and handling information security risks tailored to organizational needs. The requirements set out in ISO 27001 are general and are intended to be applicable to all organizations, regardless of type, size or nature. ISO 27001 contains control objectives covering 14 categories (Chapple, 2020, p.796) include:

a. *Information security policies*
b. *Organization of information security*
c. *Human resource security*
d. *Asset management*
e. *Access control*
f. *Cryptography*
g. *Physical and environmental security*
h. *Operations security*
i. *Communications security*

j. *System acquisition, development, and maintenance*
k. *Supplier relationships*
l. *Information security incident management*
m. *Information security aspects of business continuity management*
n. *Compliance with internal requirements, such as policies, and with external requirements, such as laws*

2.1.2 Cyber Defense

Cyber defense is an effort to overcome cyber attacks that can hinder the implementation of national defense. Cyber defense is divided into several phases: attack prevention, information security monitoring, attack analysis, defense, counterattack and information security enhancement. Cyber defense is implemented as a form of protection of Vital Information Infrastructure (IIV) in sectors which include: government administration, energy and mineral resources, transportation, finance, health, information and communication technology, food, defense and other sectors determined by the President.Cyber defense is organized through stages:

a. Attack Prevention. This stage focuses on prevention activities that have the potential to cause cyber threats or attacks.
b. Information Security Monitoring. At this stage, it is necessary to monitor the entry and exit of information that could be indicated as disrupting the stability of data security.
c. Attack Analysis. If indications of an attack are found in the previous stage, then immediately analyze the attack.
d. Defense. Based on the results of an attack that is considered dangerous or not dangerous, the next step is to carry out a defense phase to secure vital data which is at risk of causing negative impacts if it is leaked.
e. Counter-attack. Once the data has been secured, then carry out a counterattack to reduce the enemy's concentration in attacking, so that they change the focus of their attack to defending their device.
f. Increased Information Security. In between these backlashes, we can take the opportunity to improve data security.

Figure 2.2 Cyber Defense Phase
Source: Republic of Indonesia Minister of Defense Regulation No. 82 of 2014

Implementing cyber defense is an effort to protect vital information infrastructure. Vital Information Infrastructure (IIV) is an electronic system that utilizes information technology and/or operational technology, either independently or interdependently with other electronic systems in supporting strategic sectors, which if disruption, damage and/or destruction occurs to the infrastructure in question will have serious impacts. towards the public interest, public services, defense and security, or the national economy (Presidential Decree No. 82 of 2022).

In the Indonesian Cyber Security Landscape, a recapitulation of events threatening IIV in Indonesia during 2022 was recorded, namely: 399 cases of cyber threat intelligence, 27,956 cases of darknet exposure and 245 cases of data breach. From this recapitulation, several events have been predicted that will occur in the following year in the form of incidents: ransomware, data leaks, Advanced Persistent Threat (APT), phishing, cryptojacking, Distributed Denial of Service (DdoS), Remote Desktop Protocol (RDP), social engineering and web defacement.

Table 2.1 Recapitulation of Cyber Incidents in 2022

STAKEHOLDERS	CYBER THREAT INTELLIGENCE	DARKNET EXPOSURE	DATA BREACH
Government Administration	120	21,302	98
Energy and Mineral Resources	20	143	13

Information and Communication Technology	25	406	20
Defense	20	503	12
Transportation	13	17	14
Finance	14	375	13
Health	11	28	11
Food	3	14	3
Other	59	5,168	61
Total	**399**	**27,956**	**245**

Source: National Cyber and Crypto Agency (2022)

BSSN also recorded that there were 2,348 web defacement incidents that occurred on Indonesian sites, most of which occurred in January, for a total of 416 online corruption incidents. The defense sector is the second sector most affected by web defacement attacks with a total of 258 cases. Such attacks are attacks carried out to exploit a vulnerable website or web server by exploiting system vulnerabilities to allow the attacker to damage, modify, or delete the content of the compromised website.

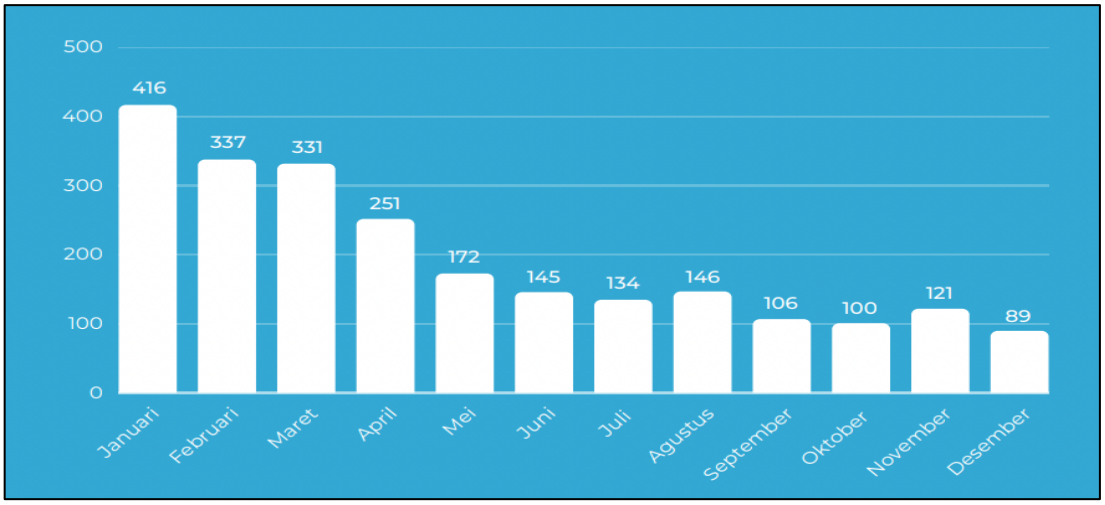

Figure 2.3 Web Defacement Attacks of 2022
Source: BSSN (2022)

Table 2.2 Web Defacement Attacks of 2022

Sector	Number of Cases
Government Administration	885
Energy and Mineral Resources	6
Information and Communication Technology	14
Defense	258
Transportation	3

Finance	6
Health	16
Food	7
Other	1153
Total	**2,348**

Source: National Cyber and Crypto Agency (2022)

Minimizing cyber threats in Indonesia that will occur in the following year requires a national cyber security strategy and cyber crisis management as follows:

1) The national cyber security strategy is implemented in the focus areas of governance, risk management, preparedness and resilience, strengthening IIV protection, national cryptographic independence, increasing capacity and quality capabilities, cyber security policy and international cooperation.
2) Cyber crisis management is carried out before, during and after a cyber crisis.

2.1.3 Web Application Firewall

WAF is a special type of firewall that operates at the application layer to filter attacks against web applicationsChapple (2020, p. 533).Chapple (2020, p. 533)explains that generally WAFs have a default rule set that references the OWASP Top 10 (owasp.org/www-project-top ten/) or other common application security risks.WAF is a system that checks traffic on web applications to filter potentially dangerous content (Harris, 2021, p.363). Due to its separate location from the web application, WAF provides an additional layer of defense that can be set independently without having to reconfigure the web application (Harris, 2021, p.363). According to Chapple (2020:77). Implementing a Web Application Firewall is an important part of protecting Web Server Security (Surya, 2023). WAF is a firewall specifically designed to protect website applications from attacks such as SQL Injection and XXS. Chapple (2020, p.495) also explains that WAF can be a defense layer solution if it is not possible to patch website applications.

WAFs consist of a variety of architectures and operating mechanisms that vary in terms of ease of WAF implementation and resulting WAF functionality. The following are several methods of using WAF according to EC-Council (2022, p.1128):

a. *Reverse proxy*

In reverse proxy mode, the WAF functions as a proxy to the application server. Therefore, device traffic goes directly to the WAF. An encrypted connection terminated at layer 7 allows the WAF to decrypt and analyze web traffic. This gives the WAF complete control over the traffic in terms of content rewriting based on security mechanisms.

b. *Layer-2 bridge*

In layer-2 bridge mode, the WAF remains parallel and acts as a layer-2 switch. WAF monitors incoming requests, performs passive Secure Sockets Layer (SSL) decryption, and blocks traffic by simply dropping packets. This mechanism provides more performance than a reverse proxy without requiring many network changes. However, it does not support content rewriting based on security mechanisms. Layer-2 bridge mode is architecturally very similar to reverse proxy mode.

c. *Out of band*

In the out-of-band method, the WAF does not remain in-line and has the least impact on the application and network. The monitoring port on the network sends a copy of incoming traffic to the WAF. Here, the WAF simply passively decrypts the SSL traffic and transfers Transmission Control Protocol (TCP) reset packets to block the traffic. Here, WAF configuration can be performed to detect malware network traffic preventing false-positive traffic intrusions, leading to application termination.

d. *Resident servers*

*Servers*Resident or embedded WAF is software that is installed on the host running the web server. It can be installed as an application or server plugin. WAFs that live on the server create additional load on the server, and do not function like their network equipment counterparts. Therefore, it is a good idea to check the server utilization resources before installing WAF.

e. *Internet*hosted/cloud

Using a cloud provider to implement WAF works like a reverse proxy mode. Here, the Domain Name System (DNS) is configured to a point in the cloud, which creates another connection to the web application. While this is increasingly becoming a popular choice for WAF deployments, it has its drawbacks. WAF implementation is not under the control of the organization, so it requires review to ensure that compliance requirements are met by the cloud provider.

The benefits of WAF that can help organizations strengthen the security of their web applications from ever-evolving threats according to EC-Council (2022, p.1129) are as follows:

a. WAF implementation secures existing and productive web applications.
b. Many WAFs have functions that can be used in the design process to minimize workload.
c. Provides cookie protection with encryption and signature methodology.
d. Secures applications against cross-site request forgery and eliminates parameter tampering with URL encryption.
e. WAF can detect data validation issues through in-depth testing of characters, character lengths, value ranges, etc.
f. WAF enables network defenders to describe compliance with regulatory standards such as Payment Card Industry (PCI), Health Insurance Portability and Accountability Act (HIPAA), and General Data Protection Regulation(GDPR).

Apart from having benefits, usesWAFalso has limitations. The following are the limitations that WAF has according toEC-Council(2022, p.1130):

a. WAF is not a replacement for proper application security solutions such as user authentication and input filtering.
b. WAF is not a technology requiring the full attention of the network administrator once implemented.
c. The way WAF works is different from Next Generation Firewall (NGFW). WAF inspects traffic based on specific protocols, unlike NGFW which can make changes to existing networks.
d. WAF does not provide complete security from all web attacks, because it cannot read database commands.

e. A WAF can prevent some problems such as session fixation and anti-automation only if the WAF manages the sessions itself.

f. Implementing a WAF does not guarantee protection against false positives.

2.1.4 SIEM

Security Information and Event Management (SIEM) is a monitoring system that is capable of detecting attacks and security system responses to attacks through log analysis from various event logs sourced from real-time data. Logs are information from a device that contains activities from the log, starting from network traffic, device status and others. (Khotimah, 2022). The architecture of this SIEM is shown in Figure 2.4.

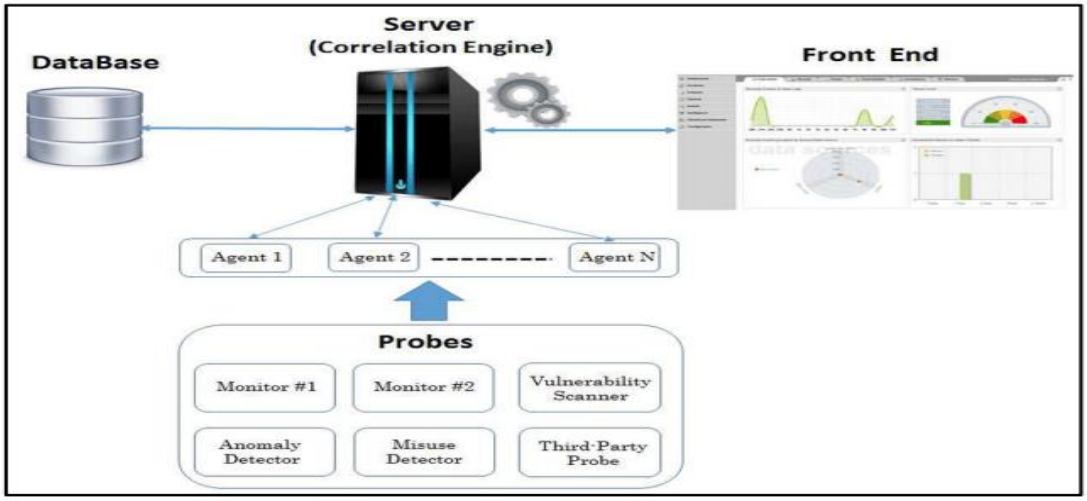

Figure 2.4 SIEM Architecture
Source: processed by researchers (2024)

SIEM systems work by gathering information from various network infrastructure sources, including network, security, servers, databases, and applications, to identify potential external and internal threats. SIEM inputs are considered to be sensors that record events based on their location. The collected data is displayed in graphical form on the dashboard to make it easier to read and understand or find special patterns. SIEM provides long-term storage so data can be correlated over time. SIEM technology can use correlation techniques that are integrated with various data sources to process data into useful information.

2.1.5 *Website*

According to A. Taufiq Hidayatullah inHamdan Romadhon & Yudhistira (2021) Websites are the most visible part of the world's largest network, namely the internet. Haer TalibinHamdan Romadhon & Yudhistira (2021) also explain that a website is a place on the internet that has a name and address. Boone in Hamdan Romadhon & Yudhistira (2021) also explains that a website is a collection of graphically rich information sources that are interconnected with each other on the larger internet. Chapple (2020, p.190) explains that websites are a commonly used tool for collecting data.

The website has a crucial role in implementing the Economic Sector Defense System (SPBE) in the Indonesian Navy. Through this digital platform, the Indonesian Navy can simplify administrative processes, manage data, and provide fast and accurate access to information related to economic aspects in the maritime environment. With SPBE, the Indonesian Navy can monitor economic activities, ensure compliance with regulations, and facilitate economic growth in the waters they handle.

In addition, the website also allows the Indonesian Navy to strengthen relationships with economic stakeholders in the region. Through communication and collaboration features on the website, the Indonesian Navy can facilitate the exchange of information, open lines of dialogue, and provide recommendations or direction regarding economic policy. This creates a conducive environment for economic growth and strengthens synergies between the defense and economic sectors.

Not only that, by utilizing the website in SPBE, the Indonesian Navy can effectively monitor and evaluate the implementation of economic activities in the waters they supervise. Data collected through the website can be processed and analyzed to evaluate economic impact, ensure sustainable use of resources, and monitor compliance with national economic policies. Thus, the website becomes an important tool in building economic defense capacity in the Indonesian Navy to support security and prosperity in the maritime area.

Harris (2021, p.362) explains that given its open nature, websites are the main target in an attack targeting information systems. In line with this, according to data obtained from Disinfolahtal's security perimeter in the period

February 2022 to September 2023, as many as2,720,027 attacks targeted websites belonging to the Indonesian Navy. Of this number, the majority of attempted attacks were identified as HTTP Signature Violation which specifically targets the http protocol used by website applications.

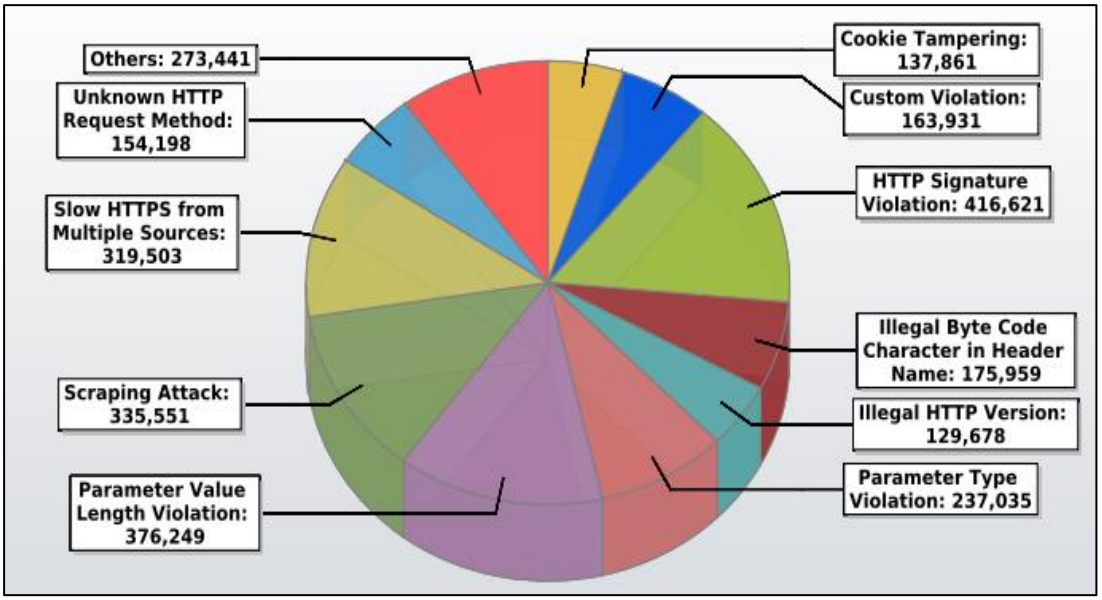

Figure 2.5 Total attack on the Indonesian Navy
Source: Disinfolahtal, 2023

2.1.6 YARA Rules

YARA rules are a set of rules used to identify and categorize malware samples. These rules are used to detect and prevent malware attacks by creating a description of the malware family. YARA rules are created by identifying unique patterns and strings in malware that allow researchers to identify threat families and malware families associated with those samples. By creating YARA rules from multiple samples from the same malware family, it is possible to identify multiple samples associated with the same campaign or threat actor. YARA rules can be used to detect malware based on similar samples. YARA rules can be used in static analysis solutions that perform decomposition, dynamic sandbox solutions that perform in-memory YARA matching, network IPS control, or even SIEM. Figure 2.6 is an example of the structure of YARA rules.

```
/*
    Yara Rule Set
    Author: YarGen Rule Generator
    Date: 2015-07-09
    Identifier: bin
*/

/* Rule Set ----------------------------------------------------------------- */

rule backdoor {
    meta:
        description = "Auto-generated rule - file backdoor.exe"
        author = "YarGen Rule Generator"
        reference = "not set"
        date = "2015-07-09"
        hash = "bad8c7e6836b9a5679bfac0bc7483091e8e168f2"
    strings:
        $s0 = "%systemroot%\\System32\\rundll32.exe \"" fullword ascii /* PEStudio Blacklist: str
        $s1 = "c:\\Agenti\\SimpleVector\\Release\\SimpleVector.pdb" fullword ascii /* score: '28.
        $s2 = "GetCurrentProcessID" fullword ascii /* PEStudio Blacklist: strings */ /* score: '2
        $s3 = "<requestedExecutionLevel level=\"highestAvailable\" uiAccess=\"false\"/>" fullword
        $s4 = "SOFTWARE\\Microsoft\\VisualStudio\\9.0\\Setup\\VS" fullword ascii /* PEStudio Blac
        $s5 = "BG:\"oMpp" fullword ascii /* score: '12.00' */
        $s6 = "vvKPP80k.mKn" fullword ascii /* score: '12.00' */
        $s7 = "<?xml version=\"1.0\" encoding=\"UTF-8\" standalone=\"no\" ?><assembly xmlns=\"u"
        $s8 = "0b55581e0a49451a01584c2a1d52232245595663182 44a41405b172e11161932" fullword ascii /
        $s9 = "SimpleVector, Version 1.0" fullword wide /* score: '9.00' */
        $s10 = "* GN3?" fullword ascii /* score: '7.00' */
        $s11 = "SIMPLEVECTOR" fullword wide /* score: '6.50' */
        $s12 = ".OcL/2" fullword ascii /* score: '6.00' */
        $s13 = "VH.IYl" fullword ascii /* score: '6.00' */
        $s14 = "uKmtnQzd78" fullword ascii /* score: '5.00' */
        $s15 = "About SimpleVector" fullword wide /* score: '5.00' */
    condition:
        uint16(0) == 0x5a4d and filesize < 3785KB and all of them
}
```

Figure 2.6 Examples of Yara Rules
Source: processed by researchers (2024)

Yara rules in this research are used to identify and categorize malware samples based on text or binary patterns. Here is some structure of Yara rules:

a. SecRule / Rules from ModSecurity in detecting malware attacks. There are four parts:

b. Variables: Defines the part of the request that should be checked.

c. Operator: Determines when rule matching should be triggered.

d. Transformation: Determines how to normalize variable data.

e. Action: Defines what to do when the rule is applied

2.1.7 ModSecurity

*ModSecurity*is a web-based firewall application or better known as WAF (Web Application Firewall). ModSecurity works by monitoring web traffic to detect dangerous threats before they reach the intended application/web. The following are the advantages and disadvantages of ModSecurity:

a. Excess :

1) *Realtime monitoring.*

2) *ModSecurity*easy to use.

3) Ease of integration with many types of web servers and third party integration (eg YARA rules to improve attack detection).

b. Lack :

a) *ModSecurity*requires additional rules to improve detection of web malware threats.

b) *ModSecurity*can take up a large amount of computer resources (RAM), if not configured properly.

2.1.8 Middle Theory

*Middle theory*is where the theory is at the mezo level or middle level which focuses on macro and micro studies (Dougherty & Pfaltzgraff 1990, 10-11). Middle range theory is a theory used to connect the gap between limited hypotheses from empiricist studies and also large theories or abstract grand theories.

This theory is used to develop testable hypotheses, not as a research organizing tool. Usually produces research models. Middle range theory is agreed to be a field that is relatively broader than a phenomenon, but does not discuss the phenomenon as a whole, but pays great attention to discipline in its construction.

a. Information Technology

Information technology is the result of human engineering in the process of storing information from the sender to the recipient so that the delivery of the information will be faster, spread more widely and stored for longer. According to the law on information and electronic transactions, information technology is a technique for collecting, preparing, processing, announcing, analyzing and/or disseminating information (NKSaufik, 2020)

b. Information Security

According to Kim and Solomon in Sawitri et al. (2022) explains that information security is a set of methodologies, practices or processes that can be carried out to protect digital information or analog information that is owned. Information security is the protection of information from confidentiality, integrity and availability when the information is being

processed, transmitted or stored. Harris (2021, p.44) also explains that the core objective of information security is to provide confidentiality, integrity and availability (CIA Triad) for each important information asset with different levels of protection according to the level of priority and vulnerability based on risk assessment calculations. .

Harris (2021, p.44) also explains that all security mechanisms and controls are implemented to provide one or more types of protection by measuring all risks, threats and vulnerabilities based on their potential ability to attack one or more of the CIA Triad.

In reality, when information security issues are addressed, it is generally only done through the lens of maintaining confidentiality (*confidentiality*). Integrity and availability threats are often ignored and only addressed after their impact is felt (Harris, 2021, p.45). It should be understood that some information assets have strict confidentiality requirements such as company trade secrets, some other assets have vital integrity requirements such as the value of financial transactions, and some have strict availability requirements such as web e-commerce.

Apart from the main aspectsCIA triad, information security cannot be separated from the term*vulnerability, threat, risk* And*exposure*.*Vulnerability* is a weakness in a system that allows threat sources to penetrate system security (Harris, 2021, p.46). Vulnerability can be in the form of software, hardware, procedural weaknesses or human errors that can be exploited. Threat is any potential danger associated with exploiting a vulnerability (Harris, 2021, p.46). Risk is the possibility of a threat source exploiting vulnerabilities and related matters that have an impact on an organization's business (Harris, 2021, p.46). For example, if a firewall has several open ports, it is likely that an intruder will use them to access the network with unauthorized methods. Another example is if an intrusion detection system (IDS) is not implemented on a network, there is a higher chance that an attack will go unnoticed until it successfully damages or steals confidential information from the server. Risk relates vulnerabilities, threats, and possible exploitation that impact an organization's business (Harris, 2021, p.46). Exposure is the

possibility of loss that an organization accepts when a risk occurs (Harris, 2021, p.46).

The existence of potential threats to information security requires security control and countermeasures. Harris (2021, p.46) explains that security control and countermeasures are all actions taken to reduce potential risks. According to Harris (2021, p.48), there are 3 main forms of security control carried out, namely administrative control, technical control and physical control. Administrative control is usually referred to as "soft control" because it is more management oriented. Examples of administrative controls are security documentation, risk management, personnel security, and training. Technical controls (also called logical controls) are software or hardware components, such as firewalls, IDS, encryption, and identification and authentication mechanisms. And physical controls are things done to protect physical facilities, personnel and resources. Examples of physical controls are security guards, locks, fences, and lighting.

2.2 Previous Research Results

In carrying out this research, the author carried out comparisons taken from several studies of other authors that had been carried out previously as a comparison for this research, shown in table 2.2. The following is a summary of each previous study that the author cites:

a. In the first research by Alvi, et al in 2022 with the title Comparative Analysis of the Performance of Web Ticketing Applications at PT Aplikanusa Lintasarta with the Implementation of ModSecurity and Shadow Daemon, it shows that the implementation of Modsec can secure the web ticketing application but does not reduce performance when accessing the application. This is shown by the performance value at a throughput of 15Kbps with a delay of 32 milliseconds. The method used in this research is the Quality of Service method with throughput and response time parameters.
b. The second research entitled Implementation and Analysis of ModSecurity on Web Based Application With OWASP Standard written by Kirana, et al in 2021 explains that the use of ModSecurity provides an effectiveness level of 66% for protecting the web from attacks on theft of

personal data.

c. The third research conducted by Imrana et all with the title, Towards a Framework of Configuring and Evaluating ModSecurity WAF on Tomcat and Apache Web Server explains that the implementation of ModSecurity WAF on Java Tomcat with JSP Language with Apache Web Server is able to provide a level of security with an accuracy of 66% .

d. In the fourth study written bySurya Yusra et all, with the title Application Firewall ModSecurity and Shadow Daemon in Apache Web Server Security, 2023 explains that the use of ModSecurity and Shadow Daemon on the web server security system can block SQL injection attacks, Cross Site Scripting (XSS), display prohibited messages and by hiding data from the user executing it. The research method used in this research is the experimental method.

e. In the fifth research by Nguyen et all, with the title Improving ModSecurity WAF Using a Structured-Language Classifier, 2021 explains thatThe use of ModSecurity development in WAF has a processing time efficiency of 0.05 seconds on the CSIC 2010 dataset.

f. In the sixth research entitled Improving Web Application Security Using Web Application Firewall (WAF) in an Integrated Campus Management Information System, it explains that the Web Application Firewall (WAF) used is ModSecurity and the Core Rule Set from OWASP as basic rules which have been successfully implemented on the information system web server. campus, this was obtained based on the author's experiments with Cross Site Scripting (XSS) and SQL Injection security holes. WAF works based on rules and a mechanism for scanning malicious scripts or requests. Apart from that, it has the ability to reject scripts or requests as a prevention of malicious attacks on web servers that contain HTTP requests in accordance with predetermined rules.

g. In the seventh study by Lakhno V, Blozva A et all with the title Experimental Studies Of The Features Of Using Waf To Protect Internal Services In The Zero Trust Structure explains that the use of WAF is a commonly used option to protect sites / applications in organizations. However, using this solution requires more flexible and personalized protection adjustments according to exact needs.

h. In the eighth research conducted by Biagio et All with the title Adversarial ModSecurity: Countering Adversarial SQL Injections with Robust Machine Learning, 2023, it was explained that the use of ModSecurity with Robust Machine Learning to handle SQL Injections provided an effectiveness level of 42% in detecting attacks.

i. Furthermore, in the ninth research conducted by Ouissem et all with the title An OWASP Top Ten Driven Survey on Web Application Protection Methods, 2020, it is explained that the use of ModSecurity is sufficient to protect websites from attacks, but it requires adjustments to the security requirements required by each application (Security SQL Inject, URL, etc)

j. In the tenth research written by Hui Yuan et all in 2019 with the title Research and Implementation of WEB Application Firewall Based on Feature Matching, it is explained that WAF development using the Feature matching method can effectively protect the web from SQL Injection attacks, XSS attacks. In this research, the method is used to retrieve attack matches with attack datasets that have been stored in the WAF database.

k. In the eleventh research conducted by Aref Shaheed, Bassam Khurdy, Web Application Firewall Using Machine Learning And Features Engineering, Hindawi Security and Communication Network Volume 2022. Explains that the use of WAF with Machine Learning and Features Engineering produces an attack accuracy of 98% in detecting attack.

Table 2.3 Previous Research

No	Researcher Name, Title, Year	Research result	Difference	Equality
1	*Alvi et all, Comparative Analysis of Web Ticketing Application Performance at PT Aplikanusa Lintasarta with the Implementation of ModSecurity and Shadow Daemon, 2022*	*The implementation carried out on web ticketing using ModSecurity is more suited to needs. This is shown in the QoS value with a bandwidth parameter of 15.45 Kb/s with an average delay of 32.59 milliseconds.*	The author compared the performance of ModSecurity with Imperva with QoS parameters	This research uses WAF ModSecurity

2	*Kirana Et All, Implementation And Analysis ModSecurity on Web Based Application With OWASP Standard, 2021*	The use of WAF ModSecurity provides web effectiveness from attacks of 66% and provides protection of privacy data on the web.	In this research, the author tested QOS performance with ModSecurity which has been adapted to the Indonesian Navy website	ModSecurity WAF testing
3	*Imrana Abdullahi et all, Towards a Framework of Configuring and Evaluating ModSecurity*WAF on Tomcat and Apache Web Server, 2019	The use of ModSecurity has proven effective in protecting PHP and JSP-based websites implemented on Apache and Tomcat servers by 67%.	This research is devoted to securing the Indonesian Navy website using PHP-based programming language and Apache Web Server	ModSecurity WAF Evaluation
4	Surya Yusra et all, Application Firewall ModSecurity and Shadow Daemon in Apache Web Server Security, 2023	In this research, this researcher will apply and analyze the security performance of a web server-based firewall application using ModSecurity and Shadow Daemon, where the aim of this web server security system research is to analyze the performance of ModSecurity and Shadow Daemon in maintaining security on the web server. Experimental method, in this research will collect data and implement a web application firewall using ModSecurity and Shadow Daemon as a web server security system and further analysis will be carried out. as a	In this research, a comparison was made between ModSecurity and Imperva in securing the Indonesian Navy website using the QoS testing method.	ModSecurity Testing

		web security server. The results of this research will show that by using ModSecurity and a Web Application Firewall based on Shadow Daemon on a web server security system you can block SQL injection attacks, Cross Site Scripting (XSS), display prohibited messages and hide data from the user who executes them.		
5	Nguyen et all, Improving ModSecurity WAF Using a Structured-Language Classifier, 2021	The use of ModSecurity Development in WAF has a processing time efficiency of 0.05seconds on the CSIC 2010 dataset	In this research, the author developed ModSecurity which has been adapted to the Indonesian Navy website and compared its performance with WAF Imperva.	This research has the same research focus on WAF ModSecurity
6	Lakhno V, Blozva A et all, EXPERIMENTAL STUDIES OF THE FEATURES OF USING WAF TO PROTECT INTERNAL SERVICES IN THE ZERO TRUST STRUCTURE	The use of WAF (Web Application Firewall) in zero-trusted systems is a commonly used option to protect sites/applications in organizations. However, using this solution requires more flexible and personalized protection adjustments according to exact needs.	The use of ModSec and Imperva WAFs is adjusted to the security needs of the Indonesian Navy website. However, this research will focus on comparing the performance between Modsec and Imperva. It is hoped that using ModSecurity can provide an alternative	Experimental use of WAF

			WAF that is quite affordable and has performance that has been adjusted to suit your needs.	
7	Increasing Web Application Security Using Web Application Firewall (WAF) in the Integrated Campus Management Information System	Based on the results of the implementation of the Web Application Firewall (WAF), the ModSecurity and Core Rule Set from OWASP as basic rules were successfully implemented on the integrated campus information system web server and as protection for the web server from attempted attacks with Cross Site Scripting (XSS) and SQL security gaps. Injection. WAF works based on rules and a mechanism for scanning malicious scripts or requests. Apart from that, it has the ability to reject scripts or requests as a prevention of malicious attacks on web servers that contain HTTP requests in accordance with predetermined rules.	The research focuses on comparing ModSecurity and Imperva tests with QoS parameters to determine WAF performance when securing the Indonesian Navy website.	WAF Testing
8	Biagio et All, Adversarial ModSecurity: Countering Adversarial SQL Injections with Robust Machine Learning, 2023	Our experiments show that AdvModSec, being trained on the traffic directed towards the protected web services, achieves a better trade- off between detection	ModSecurity testing which has been adjusted on the Indonesian Navy website and tested with WAF Imperva	ModSecurity WAF testing

		and false positive rates, improving the detection rate of the vanilla version of ModSecurity with CRS by 21%. Moreover, our approach is able to improve its adversarial robustness against adversarial SQLi attacks by 42%, thereby taking a step forward towards building more robust and trustworthy WAFs.	with the QoS Testing Method	
9	Ouissem et all, An OWASP Top Ten Driven Survey on Web Application Protection Methods, 2020	Using ModSecurity is enough to protect websites from attacks, but it requires adjustments to the security requirements required by each application (SQL Inject Security, URLs, etc.)	The focus of this research is testing the performance of the Indonesian Navy website when WAF Imperva or ModSecurity is installed	OWASP Imperva Testing And Mod Sec
10	Hui Yuan et all, Research and Implementation of WEB Application Firewall Based on Feature Matching, Springer 2019	WAF development using the Feature matching method can effectively protect the web from SQL Injection attacks, XSS attacks. In this research, the method is used to retrieve attack matches with attack datasets that have been stored in the WAF database.	The focus of this research is only testing performance based on QoS with Throughput and Responsetime parameters when installing a firewall	WAF Implementation on the Web
11	Aref Shaheed, Bassam Khurdy, Web Application Firewall Using Machine Learning And Features Engineering, Hindawi Security	development of a web application firewall model that uses machine learning and features engineering to detect common web attacks. The	The focus of this research is testing WAF using the QoS method to determine WAF performance when	Testing WAF on the web to detect Web attacks

	and Communication Network Volume 2022	proposed model achieves a high accuracy of 98.8% compared with related works. This model is able to analyze incoming requests to a web server, parse those requests to extract four features that describe parts of an HTTP request, and categorize whether the request is normal or anomalous. The model also has the ability to export WAF records as a new dataset with the ability to correct records. Administrators can train the proposed model using the exported dataset to strengthen the WAF in protecting its web applications.	implementing ModSecurity	

Based on the previous research above, studies 2, 3, 4 and 7 are the most relevant studies to the author's research. The similarity in this research from previous research is testing the performance of the Web Application Firewall. Meanwhile, the difference from previous research lies in the comparison of testing with the Imperva WAF and connecting the ModSecurity WAF with Wazuh SIEM to provide security visibility on the system. Related to this, the latest research from the author is ModSecurity Performance Testing which has been developed with YARA Rules and has been adapted to the needs of the TNI WebsiteThe Navy uses Quantitative and compares its performance with WAF Imperva.

2.3 Framework

A framework is a line of thought that facilitates research by researchers so that there is consistency between background, theory and discussion of problems. This framework makes it easier for researchers to design research materials to suit the problems and objectives of the research. The conceptual framework of this research consists of input, process, output and outcome.

In input research from data on Indonesian Navy cyber attacks from 2022 to 2023, sourced fromWAFImperva. From this input, the research process consists of theory and preliminary research, where the process produces output data on attacks on websites belonging to the Indonesian Navy. When this research model is implemented in the management of Indonesian Navy attack data, the desired result is an outcome in the form of savingsmaintenance cost.

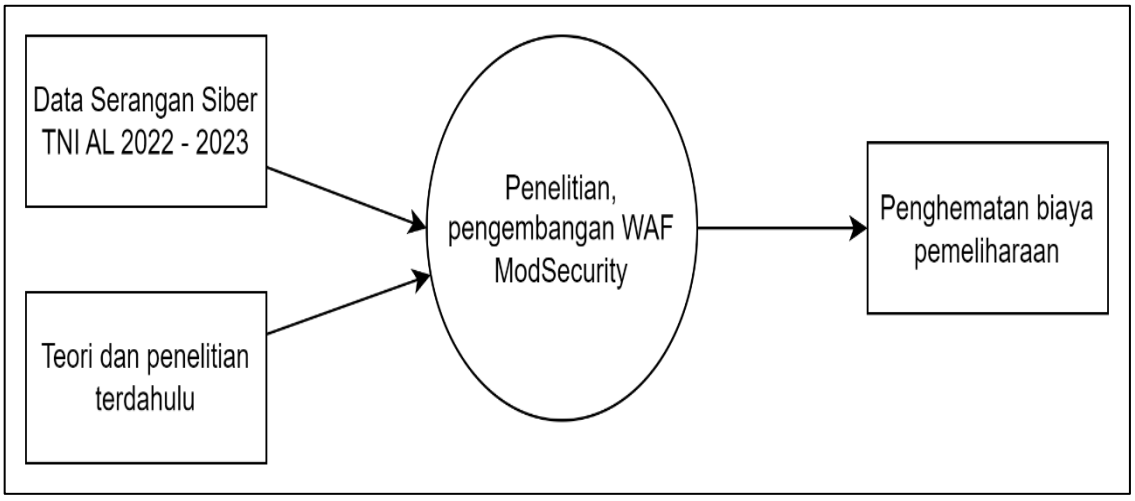

Figure 2.7 Framework
Source: processed by researchers (2024)