# Global Best Practices and Recommendations for Assessing and Improving Cybersecurity by Applying Intrusion Detection / Prevention System Selection Metrics

Veselina Gagamova[1,*], Ivo Tasev [2], Violeta Vasileva[3])
G. S. Rakovski National Defence College Sofia, Bulgaria[1]
ITWorks, Sofia, Bulgaria[2]
Future Innovation Labs[3]

v.gagamova@rndc.bg, ivo.tasev@itworks.bg, violetta.ziv@gmail.com

***Abstract:*** *This article proposes an approach to improving the use of IDS/IPS systems in computer networks of forces and means of state and local administration bodies in the event of incidents, disasters, accidents and catastrophes. To this end, good practices for selecting an appropriate type of IDPS to increase the level of cybersecurity in the organization are studied. It is proposed to use the "type" metric to develop a comparative analysis of the correspondence between the types of IDPS and their ability to protect against ransomware, using the classification of tactics and techniques in accordance with the MITRE ATT&CK framework.*
***Keywords****: METRICS, CYBERSECURITY ASSESSMENT, IDPS, MITRE FRAMEWORK*

## *1. Introduction*

In the context of rapidly evolving cyber threats and the increasing sophistication of attack vectors [5, 6, 7], organizations across the globe face the urgent challenge of maintaining resilient and adaptive cybersecurity systems. Traditional security mechanisms are no longer sufficient to ensure the integrity, confidentiality, and availability of information assets. Consequently, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) have emerged as critical components within modern cybersecurity architectures. Their efficiency, however, largely depends on the methodology applied for their evaluation, selection, and integration into complex network environments.

The development of global best practices for IDS/IPS assessment provides a systematic framework for identifying relevant performance, security, and operational metrics. These include detection accuracy, false positive and false negative rates, scalability, latency, interoperability, and cost-effectiveness. Furthermore, recommendations by leading international organizations, such as ISO/IEC, NIST, and ENISA, [3, 4, 7] highlight the importance of adopting standardized selection criteria to achieve balanced trade-offs between technical performance and organizational requirements.

This paper explores global best practices and recommendations for assessing and improving cybersecurity through IDS/IPS selection metrics. The objective is to provide a structured overview of methodologies, criteria, and evaluation models that support decision-makers in selecting optimal solutions tailored to specific risk landscapes. By synthesizing international standards, case studies, and comparative analyses [1], the study aims to contribute to the enhancement of both theoretical understanding and practical implementation of IDS/IPS or IDPS technologies in diverse organizational contexts.

## *2. Standards and Good Practices for Planning, Creating and Implementing Intrusion Prevention and Detection Systems*

There are numerous studies and publications on the planning, creation and implementation of intrusion prevention and detection systems, but for the purpose of the study, two main ones are considered, which were also used as sources.

In the international information security community, numerous studies, researches, and documents describing good practices have been conducted. For the purpose of this re, a publication by the National Institute of Standards and Technology (NIST) – SP 800-94 [4], as well as the international standard ISO/IEC 27039 "– Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS)" [2] were taken into account. The two documents have a similar purpose and largely overlap in content. The purpose of the documents is to assist organizations in selecting, configuring, and installing intrusion detection and prevention systems.

**Special Publication SP 800-94 of the US National Institute of Standards and Technology (NIST)**

The National Institute of Standards and Technology (NIST) has developed the special publication in fulfillment of its statutory responsibilities under the Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347. This publication is intended to help organizations understand intrusion detection system (IDS) and intrusion prevention system (IPS) technologies, and to help organizations design, implement, configure, secure, monitor, and maintain intrusion detection and prevention systems (IDPS). It provides practical, real-world guidance for each of the four classes of IDPS: network-based, wireless, network behavior analysis software, and host-based. The publication also provides an overview of additional technologies that can detect intrusions, such as security information and event management software. It focuses on enterprise IDPS, but much of the information in the publication is also applicable to stand-alone and small-scale IDPS deployments.

**International Standard ISO/IEC 27039** – "Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)" This standard provides guidance to assist organizations in preparing to implement intrusion detection and prevention systems (IDPS). Specifically, it addresses the selection, deployment, and operations of IDPS. It also provides background information from which this guidance is derived.

MITRE ATT&CK® [9] is a globally accessible knowledge base of tactics and techniques used maliciously, based on real-world observations. The ATT&CK knowledge base isused as a foundation for developing specific threat models and methodologies in the private sector, government, and cybersecurity product and services community.

A study of the correspondence between IDPS types and their ability to impact a ransomware attack according to the classification of tactics and techniques in the MITRE ATT&CK framework [3] is proposed and presented in [1].

The types of IPDS (Network, Wireless, Behavioral, Host) and their security functionalities can be successfully used as a metric option when selecting the appropriate IPDS for the organization's infrastructure.

## *3. The Possibilities for Improving Cybersecurity Through the Use of IDS/IPS/IDPS in Computer Networks*

The existing variety of IDPS solutions, as well as the analysis of modern threats, lead to the conclusion that improving the use of

IDPS in computer networks is a complex task. It requires a systematic approach to the analysis, design, construction and maintenance of the protection system and the prevention of intrusion. This task can be accomplished using the Deming approach, which includes the phases of planning, implementation, verification and action [8].

### *3.1. Planning*

#### *3.1.1. Risk Analysis*

Before selecting an appropriate IDPS system, an organization should conduct an information security risk assessment aimed at identifying the attacks and intrusions (threats) to which the organization's specific information systems may be vulnerable, taking into account factors such as the nature of the information used by the system and how it needs to be protected, the types of communication systems used, and other operational factors. By considering potential threats in the context of their specific information security objectives, an organization can identify controls that provide cost-effective risk mitigation. Once an IDPS is installed and operational, an ongoing risk management process should be implemented. This includes periodically reviewing the effectiveness of the controls in light of changes in the system's operations and threat environment.

Based on the security risk assessment, the organization must first determine, in order of priority, which assets need to be protected and then adapt the IDPS to this environment. To achieve this goal, it is necessary to collect, categorize and analyze the following information:

• Network diagrams and maps indicating the number and location of hosts, network entry points, and connections to external networks;
• Description of the organization's network management system;
• Operating systems for each host;
• Number and types of intermediate network devices such as routers and switches;
• Number and types of servers and dial-up connections;
• Description of any network servers, including types, configurations, application software, and versions running on each;
• Connections to external networks, including nominal bandwidth and supported protocols;

#### *3.1.2. Analysis of Current Security Measures*

After documenting the technical characteristics of the system environment, security protection the currently installed technologies should be identified. At a minimum, the following information is required:

• Demilitarized Zone (DMZ)
• Number, types, and location of firewalls and filtering routers;
• Identification of servers for authentication;
• Encryption of data and connections;
• Endpoint Detection and Response (EDR). cybersecurity solutions /Antivirus suites;
• Products for access control;
• Specialized security hardware such as cryptographic hardware;
• Virtual Private Networks (VPNs);
• Any other security technologies installed.

#### *3.1.3. Designing an IDPS Installation Procedure and Creating an IDPS Security Policy*

Once the risk analysis has been performed and the current security measures have been identified, an IDPS security policy should be defined. It should answer the following key questions:

• What information assets need to be monitored?
• What is the policy for emergency open and emergency close conditions?
• What type of IDPS is needed?
• Where can the IDPS be placed?
• What types of attacks need to be detected?
• What type of information needs to be recorded?
• What type of response or warning can be provided when an attack is detected?

#### *3.1.4. Set Metrics to Monitor*

Metrics are a management tool that allows you to set goals and track them. Metrics when using IDPS should be set to fulfill at least the following objectives:

• Measure the right indicators
• Report to the right people
• Be in the right format
• Be planned, created and reported at the right time

### *3.2. Implementation*

Based on the criteria provided in the previous point, a successful IDPS implementation can only be achieved through:
• A thorough requirements analysis that includes the security needs of the IDPS, based on a risk assessment.
• A careful selection of an IDPS implementation strategy;
• Identification of a solution that is compatible with the organization's network infrastructure, policies, and resources;
• Specialized training for the maintenance and operation of the IDPS;
• Documentation of training and rehearsal procedures for operating and responding to IDPS alerts.
• Due to the advantages and limitations of the different types of IDPS, it is necessary to consider hybrid use of the systems.

### *3.3. Check*

It is necessary to review the metrics already set at a pre-planned period of time. For this purpose, it is advisable to form a permanent working group and a formal validation process.

### *3.4. Action*

In case of deviation from the expected values of the metrics, it is necessary to carry out a partial or complete analysis of the points of the planning and execution process. The necessary corrections must be made and a new measurement must be carried out.

## *4. Metrics for Measuring the Effectiveness of Intrusion Detection and Prevention Systems .*

Measuring the effectiveness of Intrusion Detection and Prevention Systems (IDPS) is crucial for ensuring reliable protection of information systems [10]. The metrics used to evaluate the performance of these systems can be divided into several main categories:

1. **Detection Rate**: This metric measures the ability of an IDPS to identify malicious activities or threats. It is calculated as the ratio of correctly detected incidents to the total number of actual incidents. A high detection rate indicates that the system successfully recognizes and alerts about potential threats.
2. **False Positive Rate**: This is the percentage of legitimate actions that are incorrectly classified as malicious. A low false positive rate is important as it reduces unnecessary workload on administrators and minimizes the risk of disrupting normal system operations.
3. **Response Time**: This metric measures the time taken by the IDPS to respond to a detected incident. Fast response times are critical for minimizing damage and limiting the spread of an attack.
4. **Coverage**: Coverage refers to how well the IDPS can protect various parts of the network or system. It includes both physical components and types of threats that the system can detect and prevent.

5. **Throughput**: This metric measures the amount of traffic that the IDPS can process without significant delay. High throughput is important for maintaining network and system performance.

6. **Configuration Complexity**: This metric evaluates the complexity of setting up and managing the IDPS. Simpler and more intuitive interfaces allow for faster and accurate configuration, leading to more effective protection.

7. **Integration with Other Systems**: The ability of the IDPS to integrate with other security and monitoring systems is important for overall organizational protection. Good integration facilitates information sharing and coordinated actions.

8. **Cost of Implementation and Maintenance**: This includes both initial costs for purchasing and installing the IDPS, as well as ongoing costs for maintenance, updates, and staff training. Minimal costs while maximizing efficiency are desirable.

Using a combination of these metrics provides a comprehensive view of the effectiveness of IDPS and helps organizations make informed decisions regarding their implementation and optimization.

There are many IDS/IPS systems, but they are not sufficient as a separate product to guarantee a very high level of security for the computer networks of the forces and means of the state and local administration bodies in the event of incidents, disasters, accidents and catastrophes. A lot of money is invested in developing new attacks or masking already known ones. Weak international cooperation on cybercrime issues leads to a very low level of detection and punishment. Information assets, both of individuals and entire organizations, will increasingly be the subject of attacks.

Good practices and recommendations for assessing and improving cybersecurity would be to combine IDS/IPS with other systems supporting information security such as:

- File integrity checkers
- Firewalls
- Honeypots
- Network management tools
- Security Information and Event Management (SIEM)
- End Point Detection and Response (EDR) solutions
- Vulnerability assessment tools

## *5. Conclusion*

In conclusion, it can be summarized that In conclusion, it can be summarized that the process of improving the use of IPS/IDS in an organization by state and local administration bodies in the event of incidents, disasters, accidents and catastrophes requires in-depth work and commitment of managers and all responsible persons. There is no technical solution, software or hardware, that can guarantee absolute security. The process of planning the implementation of the solution is extremely important and it must be economically justified.. It is necessary to take into account many factors.

Metrics for measuring the effectiveness of intrusion detection and prevention systems when using IDPS should be prepared in advance. The process of checking and updating IDS/IPS should be constant, using the metrics for selecting a suitable IPDS system depending on its type.

## *Acknowledgements*

This report was written thanks to funding from the Ministry of Education and Science in implementation of the National Strategy for Research Development 2017-2030 under the National Scientific Programme "Security and Defence", adopted by Decision of the Council of Ministers No. 731 of 21 October 2021.

## *6. References*

1. Veselina Aleksandrova, Ivo Tasev, Violeta Vasileva, Challenges In Choosing The Type of Intrusion Detection and Prevention System to Increase the Level of Cybersecurity in the Organization, 12th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education (ICAICTSEE – 2022), December 02-03rd, 2022, Publishing Complex – UNWE, Sofia, Bulgaria. Volume: 50, ISSN 2367-7635 (PRINT), ISSN 2367-7643 (ONLINE), Issued for publication: June 27th, 2024 pp. 27-33, https://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2022.pdf
2. Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS) - ISO/IEE 27039 2015.02.15
3. Information technology – Security techniques – Information security management systems – Requirements ISO/IEE 270001:2015
4. National Institute of Standards and Technology - Guide to Intrusion Detection and Prevention Systems (IDPS) – Special Publication 800-94
5. ENISA – ENISA THREAT LANDSCAPE 2021
6. ENISA – ENISA THREAT LANDSCAPE 2022
7. ENISA – ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS 2022
8. Cybersecurity & Infrastructure Security Agency CISA – "Plan, Do, Check, Act" Nov 01 2013
9. https://attack.mitre.org/
10. Kumar, Gulshan. (2015). Evaluation Metrics for Intrusion Detection Systems-A Study. International Journal of Computer Science and Mobile Applications. 11.