NSS
Neutrosophic Sets and Systems, Vol. 93, 2025
University of New Mexico

Neutrosophic Measure-Integral Model for Advanced Cybersecurity Solutions Using Artificial Intelligence and Soft Computing Techniques

Mahmoud M. Ismail[1], Ahmed A. Metwaly[2], Osama ElKomy[3],Alaa Al-Ghamry [2], and Eman Sayed[1]

[1]Decision Support Department, Faculty of Computers and Informatics, Zagazig University, Zagazig, 44519, Egypt, mmsba@zu.edu.eg, essayed@fci.zu.edu.eg
[2]Department of Computer Science, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt, a.metwaly23@fci.zu.edu.eg.

[3]Department of Information Technology, Faculty of Computers and Informatics, Zagazig University, Zagazig 44519, Egypt, omelkomy@fci.zu.edu.eg.

Abstract
Cybersecurity analytics must decide under uncertainty: incomplete fields, delayed enrichment, and conflicting AI detectors are common. This work presents a mathematically rigorous neutrosophic measure-integral framework that retains three facets of evidence throughout modeling and evaluation: support t, indeterminacy i, and conflict f. On a measurable space (Ω, Σ), a neutrosophic measure is a triple $\nu(A) = (t(A), i(A), f(A)) \in \mathbb{R}^3$ which generalizes classical measure to settings with indeterminacy and enables a corresponding neutrosophic integral $\int g \, d\nu$ for Al and soft-computing scores $g[1,2]$. The study derives neutrosophic precision and recall together with risk bounds that separate deterministic error from the explicit price of i and f. A case study on enterprise email security (1,000 alerts) provides end-to-end computation: the proposed penalized neutrosophic precision improves from 0.6224 to 0.6952 after a feasible 20% reduction in indeterminacy on predicted positives; the risk upper bound tightens from 0.2369 to 0.2309. The approach plugs naturally into Advanced Cybersecurity Solutions Using Artificial Intelligence and Soft Computing Techniques by mapping neural scores, fuzzy memberships, and ensemble disagreement into (t, i, f) while preserving interpretability and providing provable guarantees.

Keywords: AI-driven cybersecurity; fuzzy logic; intrusion/phishing detection; neutrosophic integral; neutrosophic measure; performance bounds; risk decomposition; soft computing; uncertainty quantification.

1.Introduction

In the rapidly evolving landscape of cybersecurity, organizations face an unprecedented spectrum of threats, ranging from sophisticated phishing attacks and malware intrusions to advanced persistent threats that exploit vulnerabilities in networked systems. The operational tempo is high, the data are heterogeneous, and the decision context frequently involves incomplete fields, delayed enrichment from external intelligence sources, and disagreement among automated detectors. Within this environment, the integration of Artificial Intelligence (AI) and soft computing techniques has emerged as a critical strategy for enhancing detection, response, and mitigation capabilities. As highlighted in the title, "Neutrosophic Measure-Integral Model for Advanced

Cybersecurity Solutions Using Artificial Intelligence and Soft Computing Techniques," this paper proposes a novel framework that addresses the inherent uncertainties in cyber threat analytics by leveraging neutrosophic mathematics. Traditional approaches often collapse complex evidence into simplistic probabilities, leading to obscured insights and suboptimal decision-making, particularly when dealing with incomplete data, delayed information enrichment, or conflicting outputs from AI detectors [3][4]. By preserving the distinct facets of evidence, namely support, indeterminacy, and conflict, throughout the modeling process, the proposed framework yields a more nuanced and interpretable evaluation and consequently enhances the reliability of cybersecurity solutions.

The challenges in modern cybersecurity stem from the dynamic nature of threats and the limitations of conventional tools. AI-driven systems, such as deep learning classifiers and ensemble models, have revolutionized threat detection by processing vast datasets in real-time. However, they frequently encounter issues like high false positive rates and difficulties in handling ambiguous inputs [7][16]. Soft computing techniques, including fuzzy logic and evolutionary algorithms, offer flexibility in managing uncertainty. Yet they often fail to explicitly quantify conflicting evidence or indeterminacy arising from missing attributes, such as reputation scores or sandbox analysis results [9][23]. For example, in enterprise email security systems, raw event data often arrives incomplete, missing critical metadata fields. This incompleteness can lead to conflicting assessments from different AI detection components, making it challenging to consolidate their outputs into coherent, actionable insights [11][18]. This uncertainty leads to several operational inefficiencies, including the need for lengthy manual investigations and the misallocation of valuable resources. Additionally, it escalates risks considerably in critical sectors like healthcare and finance. In these areas, any delay or mistake in response can result in severe data breaches and the exposure of highly sensitive information [12][20].

A comprehensive literature review reveals a growing body of research on AI and soft computing applications in cybersecurity, with a focus on uncertainty quantification and risk management. Early works emphasized fuzzy logic for intrusion detection, demonstrating its efficacy in modeling vague boundaries between benign and malicious activities [23][24]. More recent studies have explored machine learning paradigms, such as generative AI for simulating threats and enhancing training datasets, which improve model robustness against evolving attacks [9][17][19]. For example, Ferrag and Shu [16] surveyed intrusion detection systems powered by AI, highlighting challenges in scalability and adversarial resilience. Similarly, Sarker [19] examined generative AI's role in addressing cybersecurity threats, underscoring its potential for predictive modeling while warning of risks like AI-generated deepfakes. In parallel, neutrosophic sets have gained traction as an extension of fuzzy and intuitionistic fuzzy sets, providing a tripartite structure to capture truth, falsity, and indeterminacy in decision-making processes [1][2][4][6][10].

Neutrosophic applications in cybersecurity have particularly advanced in areas like risk assessment and game-theoretic modeling of attacks. Agrawal et al. [4] introduced interval neutrosophic matrix games to counter uncertainties in cyber environments, offering a framework for strategic defense against indeterminate threats. Building on this, Abdel-Basset et al. [10] proposed neutrosophic CODAS methods for supplier assessment in supply chains, which can extend to evaluating cybersecurity vendors amid conflicting criteria [6][12]. Studies on power management and cloud security have integrated neutrosophic multi-criteria decision-making (MCDM) to prioritize risks, such as in Salama et al. [13], where machine learning models incorporate neutrosophic numbers for anomaly detection in networks [14][15]. Yadav [6] applied neutrosophic AHP to analyze Industry 4.0 technologies' impact on sustainability, including cybersecurity implications, while Alshammari [14] used TODIM and PROMETHEE in neutrosophic frameworks for cloud security measures. These works collectively demonstrate neutrosophic sets' superiority in handling

indeterminacy over traditional fuzzy approaches, as evidenced in violence detection and infrastructure defense models [5][9].

Further integrating AI with neutrosophic theory, recent contributions address performance bounds and risk decomposition. Abdel-Basset et al. [15] developed MCDM methodologies for cyber risks in power systems, decomposing uncertainties into quantifiable components [21][22]. Mahajan [11] reviewed AI's leverage in cybersecurity, emphasizing explainable models for resilient applications [18][24]. Koch et al. [22] outlined process models for implementing AI in cybersecurity, incorporating risk bounds to ensure operational guarantees. In threat modeling, Sujatha et al. [5] modeled attack-defense games using fuzzy graphs with neutrosophic elements, while Sharma et al. [25] proposed AI-based automated systems with computational bounds for alert management. Alqahtani et al. [3] provided a comprehensive review of AI-driven detection, aligning with soft computing's role in uncertainty handling [7][8]. Apruzzese et al. [23] and Wang et al. [24] systematically analyzed AI's impacts on augmentation and assurance, revealing gaps in explicit indeterminacy modeling that our framework addresses [20][21]. Overall, while these studies, spanning over 25 key references, advance the field, they often lack a unified measure theoretic approach that preserves all uncertainty facets through integrals and provides provable bounds [1][2][13][16][17][19].

This paper bridges these gaps by introducing a rigorous neutrosophic measure-integral framework tailored for AI and soft computing in cybersecurity. Our contributions include: (i) A self-contained measure-theoretic foundation with definitions, properties, and integrals for neutrosophic modeling [1][2]; (ii) Novel performance metrics like neutrosophic precision/recall and penalized variants that explicitly account for indeterminacy and conflict [4][6]; (iii) Additive risk bounds via Theorem 1, decomposing errors into deterministic and uncertainty-driven components [15][20]; (iv) A practical case study on 1,000 email alerts, demonstrating end-to-end computations and sensitivity analysis [3][11]; and (v) Implementation recipes mapping soft computing outputs to neutrosophic triples, enabling auditing and enrichment [9][18][23]. The framework aligns with advanced cybersecurity solutions by preserving interpretability and offering guarantees absent in prior works [7][12][22].

The remainder of the paper is organized as follows: Section 2 presents preliminaries on measurable structures and neutrosophic measures. Section 3 defines performance functionals and risk bounds. Section 4 details the case study with computations. Section 5 provides implementation guidelines. Section 6 discusses implications, and Section 7 concludes.

2. Preliminaries

This section establishes the mathematical foundation for our neutrosophic framework by introducing the core concepts of measurable structures, neutrosophic measures, integrals, and decision regions. Each concept builds systematically toward the practical evaluation methodology presented in later sections.

2.1 Basic measurable structure

Definition 2.1 (Cyber Event Space). Let Ω represent the universe of cyber events under analysis, where each element $\omega \in \Omega$ corresponds to a specific security event such as an email message, network flow, system log entry, or security alert. We equip Ω with a σ-algebra Σ, forming a measurable space (Ω, Σ).

The σ-algebra Σ is a collection of subsets of Ω that satisfies three fundamental properties: (i) $\Omega \in \Sigma$, (ii) if $A \in \Sigma$, then $\Omega \setminus A \in \Sigma$, and (iii) for any countable collection $\{A_i\} \geq 1 \subset \Sigma$, we have $\bigcup_i \geq$

$1, A_i \in \Sigma$ This structure ensures that all relevant subsets of events are measurable and can be assigned neutrosophic masses.

Example 2.1. In enterprise email security, Ω might represent all incoming messages over a fixed time period, while Σ includes all possible combinations of event attributes such as sender reputation categories, attachment types, or content classification results.

2.2 Neutrosophic measure

Definition 2.2 (Neutrosophic Measure). A neutrosophic measure on the measurable space (Ω, Σ) is a mapping

$$\nu: \Sigma \to \mathbb{R}^3, \nu(A) = (t(A), i(A), f(A))$$

where each component $t, i, f: \Sigma \to R \geq 0$ represents a finite, countably additive measure.

The three components have distinct semantic interpretations in cybersecurity contexts:

Support $t(A)$: The mass of evidence supporting the hypothesis that events in set A are malicious

Indeterminacy $i(A)$: The mass of evidence that is inconclusive or ambiguous regarding events in A

Conflict $f(A)$: The mass of evidence supporting the hypothesis that events in A are benign

Property 2.1 (Countable Additivity). For any pairwise disjoint sequence $\{A_k\}_{k\geq 1} \subset \Sigma$, each component satisfies:

$$t\left(\bigsqcup_{k\geq 1} A_k\right) = \sum_{k\geq 1} t(A_k), i\left(\bigsqcup_{k\geq 1} A_k\right) = \sum_{k\geq 1} i(A_k), f\left(\bigsqcup_{k\geq 1} A_k\right) = \sum_{k\geq 1} f(A_k)$$

Property 2.2 (Standard Measure Properties). Each component *t*,*i*,*f* inherits standard measure-theoretic properties:

1. **Null Empty Set**: $t(\emptyset) = i(\emptyset) = f(\emptyset) = 0$
2. **Monotonicity**: If $A \subseteq B$, then $t(A) \leq t(B)$, $i(A) \leq i(B)$, and $f(A) \leq f(B)$
3. **Continuity from Below**: For an increasing sequence $A_1 \subseteq A_2 \subseteq \cdots$, we have $\lim_{n\to\infty} \mathrm{t}(A_n) = \mathrm{t}(\bigcup_{\mathrm{n}=1}^{\infty} A_n)$, and similarly for *i* and *f*
4. **Continuity from Above**: For a decreasing sequence $A1 \supseteq A2 \supseteq \cdots$ with $t(A_1) < \infty$, we have $\lim_{n\to\infty} \mathrm{t}(A_n) = t(\bigcap_n = 1\infty A_n)$, and similarly for *i* and *f*

Remark 2.1. The neutrosophic measure framework generalizes classical probability measures and fuzzy measures by explicitly modeling uncertainty through the indeterminacy component *i* and conflicting evidence through the component *f*. When $i \equiv 0$ and f is ignored, the framework reduces to classical measure theory [1]. When $f \equiv 0$, it reduces to intuitionistic fuzzy measures.

2.3 Neutrosophic integral (component lift)

Definition 2.3 (Neutrosophic Integral). Given a measurable function $g: \Omega \to [0,1]$ representing a security score (such as a neural network output, fuzzy membership value, or ensemble confidence), the neutrosophic integral with respect to measure ν is defined component-wise as

$$\int g \, \mathrm{d}\nu \triangleq (\underbrace{\int g \, \mathrm{d}t}_{\text{support}}, \underbrace{\int g \, \mathrm{d}i}_{\text{indeterminacy}}, \underbrace{\int g \, \mathrm{d}f}_{\text{conflict}})$$

compatible with the neutrosophic integral viewpoint where indeterminacy can arise in the function, the limits, or the underlying space $[1,2]$, where each component integral follows the standard Lebesgue integration theory.

Interpretation. The neutrosophic integral provides a comprehensive aggregation mechanism that preserves all three facets of evidence throughout the integration process. Unlike classical approaches that collapse uncertainty into point estimates, this formulation maintains the distinction between supportive evidence, indeterminacy, and conflict at every computational step.

2.4 Decision regions and confusion cells

Definition 2.4 (Decision Threshold and Regions). Fix a decision threshold $\tau \in (0,1)$. For a measurable detector score function $s: \Omega \to [0,1]$, define the predicted decision regions:

$$\text{PredPos} = \{\omega \in \Omega : s(\omega) \geq \tau\}, \ \text{PredNeg} = \Omega \setminus \text{PredPos},$$

and let $\text{Pos}, \text{Neg} \subset \Omega$ denote the ground-truth positive and negative sets, respectively, with $Pos \cup Neg = \Omega \; and \; Pos \cap Neg = \emptyset$.

Definition 2.5 (Neutrosophic Confusion Cells). The neutrosophic confusion matrix is defined through four measurable sets:

$$\text{TP} = \text{PredPos} \cap \text{Pos}, \text{(True Positives)}$$

$$\text{FP} = \text{PredPos} \cap \text{Neg}, \text{(False Positives)}$$

$$\text{FN} = \text{PredNeg} \cap \text{Pos}, \text{(False Negative)}$$

$$\text{TN} = \text{PredNeg} \cap \text{Neg}, \text{(True Negative)}$$

each carrying a triple $\nu(\cdot)$.

Each cell carries a neutrosophic triple $\nu(\cdot) = (t(\cdot), i(\cdot), f(\cdot))$, providing a complete characterization of the evidence distribution across decision outcomes.

Property 2.3 (Partition Property). The confusion cells form a partition of Ω:

$$TP \cup FP \cup FN \cup TN = \Omega$$

and the sets are pairwise disjoint.

Remark 2.2. Unlike classical confusion matrices that only capture event counts, neutrosophic confusion cells preserve the complete evidence structure within each decision category. This enables fine-grained analysis of where uncertainty and conflict concentrate, providing actionable insights for system improvement.

Example 2.2. In malware detection, the TP cell might contain high support masses $t(TP)$ for confidently detected threats, while the FP cell might show elevated indeterminacy $i(FP)$ indicating borderline cases that require additional analysis. The FN cell could reveal conflict masses $f(FN)$ where benign evidence incorrectly dominated, suggesting calibration issues in the detection system.

This mathematical foundation provides the necessary tools for defining neutrosophic performance metrics and risk bounds in the following section, ensuring that all uncertainty facets are preserved and quantified throughout the evaluation process.

3. Neutrosophic performance and risk

This section develops performance metrics and risk bounds that leverage the full neutrosophic structure established in Section 2. Unlike classical evaluation approaches that collapse uncertainty into point estimates, our framework maintains explicit separation between deterministic errors and the quantifiable costs of indeterminacy and conflict throughout the evaluation process.

3.1 Neutrosophic precision/recall

Definition 3.1 (Basic Neutrosophic Performance Metrics). Using the neutrosophic confusion cells from Definition 2.5, we define neutrosophic precision and recall based solely on supportive evidence masses:

$$P_N \triangleq \frac{t(\mathrm{TP})}{t(\mathrm{TP}) + t(\mathrm{FP})}, R_N \triangleq \frac{t(\mathrm{TP})}{t(\mathrm{TP}) + t(\mathrm{FN})}$$

Interpretation. These metrics focus exclusively on the supportive component *t* of the neutrosophic measure, providing a conservative assessment of system performance based only on confident evidence. This approach ensures that uncertain or conflicting evidence does not artificially inflate performance estimates.

Definition 3.2 (Penalized Neutrosophic Precision). To explicitly account for uncertainty and conflict in predicted positive decisions, we define a penalized precision metric:

$$P_N^{(\gamma,\delta)} \triangleq \frac{t(\mathrm{TP})}{t(\mathrm{TP}) + t(\mathrm{FP}) + \gamma i(\ \mathrm{PredPos}\ ) + \delta f(\ \mathrm{PredPos}\ )},$$

with $\gamma, \delta \geq 0$, are user-configurable penalty coefficients and $PredPos = TP \cup FP$ represents all predicted positive events.

3.2 Neutrosophic risk and an additive bound

Let $\ell \in [0,1]$ be a 0 - 1-like loss. We define the neutrosophic risk

$$\mathcal{R}_N \triangleq \frac{1}{N}(\underbrace{\mathrm{FP} + \mathrm{FN}}_{\text{deterministic error}} + \alpha I + \beta F)$$

where $N = |\Omega|$ (finite sample), $I \triangleq i(\Omega), F \triangleq f(\Omega)$, and $\alpha, \beta \geq 0$ encode loss sensitivity to indeterminacy and conflict.

Theorem 1 (Additive uncertainty bound).
For any $\alpha, \beta \geq 0$,

$$\mathcal{R}_N \leq \mathcal{R}_{\text{det}} + \frac{\alpha I + \beta F}{N}, \mathcal{R}_{\text{det}} \triangleq \frac{\text{FP} + \text{FN}}{N}$$

Proof. Decompose $v(\Omega) = (T, I, F)$. The loss contribution from determinate support aligns with classical errors FP + FN. The contributions from I and F are upper-bounded by αI and βF by construction of ℓ and calibration of α, β. Dividing by N yields the claim.

Discussion. When $I = F = 0$ (no indeterminacy/conflict), $\mathcal{R}_N = \mathcal{R}_{\text{det}}$ and neutrosophic evaluation reduces to classical evaluation intended generalization property [1].

4. Case Study

This section demonstrates the practical application of our neutrosophic framework through a comprehensive case study of an enterprise email security system. We model a realistic scenario in enterprise email system where an AI ensemble (deep classifier + fuzzy rules + evolutionary weighting) assigns a score $s \in [0,1]$ to each message. Let evidence quality $q \in [0,1]$ measure coverage/metadata completeness, and model disagreement $\kappa \in [0,1]$ measure variance across detectors. We map each event to a neutrosophic triple (t, i, f):

$$t = q \cdot 2\max(0, s - 0.5), f = q \cdot 2\max(0, 0.5 - s), i = \min\left(1, (1 - q) + \frac{1}{2}\kappa\right)$$

This mapping (i) keeps t, f within [0,1] by scaling with q, (ii) treats ambiguity and disagreement as indeterminacy i, and (iii) is consistent with neutrosophic modeling of determinate/indeterminate parts [1,2]. The case study illustrates how our framework captures and quantifies the uncertainty inherent in real-world cybersecurity operations, providing actionable insights for system improvement and resource allocation.

Setting for System Configuration and Group Characteristics:

Total $N = 1000$ emails. Ground truth: 300 malicious (Pos), 700 benign (Neg). Use threshold $\tau = 0.60$ (predict malicious if $s \geq \tau$). Groups (counts and parameters) follow realistic patterns in AI-security plans using soft computing [3]:

Malicious Messages (Ground Truth Positive):
$\mathrm{G}_1 n = 180$: $(s, q, \kappa) = (0.85, 0.90, 0.20)$ (high-confidence)
$\mathrm{G}_2 n = 90$: (0.65,0.70,0.30) (borderline)
$\mathrm{G}_3 n = 30$: (0.40,0.80,0.20) (missed)

Benign Messages (Ground Truth Negative):
$\mathrm{H}_1 n = 70$: (0.75,0.60,0.40) (false-alarm-prone)
$\mathrm{H}_2 n = 140$: (0.55,0.60,0.30) (near threshold)
$\mathrm{H}_3 n = 490$: (0.20,0.90,0.10) (clearly benign).

4.1 Per-group triples (using (M))

The neutrosophic mapping formula (M) is applied to each behavioral group, transforming the raw AI scores and metadata quality indicators into structured evidence triples. The resulting triples reveal how uncertainty manifests differently across various message types and detection scenarios. These individual-level triples serve as the foundation for subsequent aggregation and cell-level analysis. From the mapping formula (M) we compute the normalized neutrosophic triples for representative emails in each group:

$\mathrm{G}_1: t = 0.63, i = 0.20, f = 0$

$\mathrm{G}_2: t = 0.21, i = 0.45, f = 0$

$\mathrm{G}_3: t = 0, i = 0.30, f = 0.16$

$\mathrm{H}_1: t = 0.30, i = 0.60, f = 0$

$\mathrm{H}_2: t = 0.06, i = 0.55, f = 0$

$\mathrm{H}_3: t = 0, i = 0.15, f = 0.54$

In Table 1, Values are computed by (M) directly from (s, q, κ). These normalized masses are later aggregated over counts to produce cell-level statistics used by neutrosophic precision/recall and risk.

Table 1 Per-group neutrosophic triples (single email)

Group	s	q	κ	t	i	f
$\mathbf{G_1}$	0.85	0.90	0.20	0.63	0.20	0.00
$\mathbf{G_2}$	0.65	0.70	0.30	0.21	0.45	0.00
$\mathbf{G_3}$	0.40	0.80	0.20	0.00	0.30	0.16
$\mathbf{H_1}$	0.75	0.60	0.40	0.30	0.60	0.00
$\mathbf{H_2}$	0.55	0.60	0.30	0.06	0.55	0.00
$\mathbf{H_3}$	0.20	0.90	0.10	0.00	0.15	0.54

4.2 Decisions and classical counts

The detection threshold $\tau = 0.60$ is applied to generate classical confusion matrix counts, establishing a baseline for comparison with our neutrosophic approach. We examine how traditional binary classification partitions the email groups and compute standard performance metrics that ignore the underlying uncertainty structure. This classical analysis provides the deterministic component of our risk decomposition while highlighting the limitations of uncertainty-blind evaluation methods.

With threshold $\tau = 0.60$: $\mathrm{TP} = \mathrm{G}_1 + \mathrm{G}_2 = 270, \mathrm{FN} = \mathrm{G}_3 = 30, \mathrm{FP} = \mathrm{H}_1 = 70, \mathrm{TN} = \mathrm{H}_2 + \mathrm{H}_3 = 630$. Classical metrics:

$$\text{Precision } = \frac{270}{270 + 70} = 0.7941, \text{ Recall } = \frac{270}{300} = 0.9000, F_1 = \frac{2PR}{P + R} \approx 0.8436.$$

These metrics provide a conventional view of system performance but fail to capture the significant uncertainty variations across different message groups, as revealed by the neutrosophic triples in Section 4.1.

4.3 Neutrosophic confusion matrix (aggregated triples)

We aggregate the neutrosophic triples additively over all events within each cell, leveraging the countable additivity property of neutrosophic measures. For each cell C ∈ {TP, FP, FN, TN}, the total masses are computed. Table 2 replaces integer counts with mass totals of (t, i, f). These are sufficient statistics for integral-based performance and risk. They show where uncertainty lives (e.g., large i on predicted positives).

Table 2 Neutrosophic confusion matrix totals.

Cell	Count	t total	i total	f total
$\mathbf{TP}(\mathbf{G_1}+\mathbf{G_2})$	270	$180 \cdot 0.63 + 90 \cdot 0.21 = 132.30$	$180 \cdot 0.20 + 90 \cdot 0.45 = 76.50$	0.00
FP ($\mathbf{H_1}$)	70	$70 \cdot 0.30 = 21.00$	$70 \cdot 0.60 = 42.00$	0.00
FN ($\mathbf{G_3}$)	30	0.00	$30 \cdot 0.30 = 9.00$	$30 \cdot 0.16 = 4.80$
TN ($\mathbf{H_2}+\mathbf{H_3}$)	630	$140 \cdot 0.06 + 490 \cdot 0 = 8.40$	$140 \cdot 0.55 + 490 \cdot 0.15 = 150.50$	$490 \cdot 0.54 = 264.60$

The global mass summations across all cells are:

$$T = \sum t = 161.70, I = \sum i = 278.00, F = \sum f = 269.40.$$

4.4 Neutrosophic performance and risk (computed)

We compute both classical and neutrosophic performance metrics to demonstrate the additional insights provided by our uncertainty-aware framework. We calculate neutrosophic precision and recall based on support masses, apply penalty coefficients to account for uncertainty costs, and derive risk bounds using our additive uncertainty theorem.

Using the aggregated masses from Table 2, we compute the neutrosophic performance metrics:

$$P_N = \frac{132.30}{132.30 + 21.00} = 0.8630, R_N = \frac{132.30}{132.30 + 0.00} = 1.0000.$$

Penalized (choose $\gamma = \delta = 0.5$):

$$i(\text{ PredPos }) = 76.50 + 42.00 = 118.50, f(\text{ PredPos }) = 0.00,$$
$$P_N^{(0.5,0.5)} = \frac{132.30}{132.30 + 21.00 + 0.5 \cdot 118.50} = \frac{132.30}{212.55} = 0.6224.$$

Neutrosophic risk bound (Theorem 1) with $\alpha = \beta = 0.25$:

$$\mathcal{R}_{\text{det}} = \frac{70 + 30}{1000} = 0.1000, \mathcal{R}_N \leq 0.1000 + 0.25\left(\frac{278.00 + 269.40}{1000}\right) = 0.2369$$

Table 3 Classical vs. neutrosophic performance

Metric	Value
Classical Precision	0.7941
Classical Recall	0.9000
Classical $\boldsymbol{F_1}$	0.8436
$\boldsymbol{P_N}$ (neutrosophic)	0.8630
$\boldsymbol{R_N}$ (neutrosophic)	1.0000

$P_N^{(0.5,0.5)}$	0.6224

The comparison in Table 3 reveals how traditional metrics can provide misleading assessments when significant uncertainty is present in the decision process. The results demonstrate that while neutrosophic recall achieves perfect performance (1.0000) based on support masses, the penalized precision (0.6224) is significantly lower than classical precision (0.7941), reflecting the substantial uncertainty costs in predicted positive decisions. This discrepancy highlights the importance of uncertainty-aware evaluation in operational cybersecurity systems.

4.5 What-if analysis (indeterminacy reduction)

Assume enrichment (e.g., sandbox verdict, domain age) shifts 20% of i (PredPos) to TP support:

$$\Delta i = 0.20 \times 118.50 = 23.70 \Rightarrow t(\text{TP}) \leftarrow 132.30 + 23.70 = 156.00, i(\text{ PredPos }) \leftarrow 94.80, I \leftarrow 278.00 - 23.70 = 254.30.$$

Updated penalized precision and bound:

$$P_{N,\text{ new}}^{(0.5,0.5)} = \frac{156.00}{156.00 + 21.00 + 0.5 \cdot 94.80} = \frac{156.00}{224.40} = 0.6952,$$

$$\mathcal{R}_{N,\text{ new}} \leq 0.1000 + 0.25\left(\frac{254.30 + 269.40}{1000}\right) = 0.2309$$

Even modest clarification of predicted positives yields measurable gains in precision and tighter risk bounds. This quantifies the return on investment for data-quality efforts and ensemble calibration in AI-driven security, as illustrated in Table 4.

Table 4 Sensitivity to indeterminacy reduction (predicted positives)

$i \to t$ shift	$P_N^{(0.5,0.5)}$	$\mathcal{R}_N$ bound
0%	0.6224	≤ 0.2369
10%	0.6600	≤ 0.2339
20%	0.6952	≤ 0.2309

5. Implementation

This section is a complete, self-contained recipe you can deploy as-is. It turns raw outputs from an Al + softcomputing ensemble into neutrosophic analytics, with every step defined and numerically verified on a small batch. Everything is expressed as paragraphs and equations; there are no undefined quantities and no external dependencies.

Inputs and basic setup. Consider a finite batch of events $\Omega = \{\omega_1, \ldots, \omega_6\}$. Each event is processed by three base detectors whose scores lie in $[0,1]$. Their arithmetic mean is the calibrated ensemble score.

$$s(\omega) = \frac{s_1(\omega) + s_2(\omega) + s_3(\omega)}{3} \in [0,1]$$

Decisions use a fixed threshold $\tau = 0.60$: predicted malicious if $s(\omega) \geq \tau$, otherwise predicted benign. Ground truth labels: 1 for malicious, 0 for benign.

Feature quality q. Let the required features be $\mathcal{F} = \{\mathrm{A}, \mathrm{B}, \mathrm{C}\}$ with importance weights $(w_{\mathrm{A}}, w_{\mathrm{B}}, w_{\mathrm{C}}) = (0.5, 0.3, 0.2)$ and presence flags $c_f(\omega) \in \{0,1\}$. Define

$$q(\omega) = \sum_{f \in \mathcal{F}} w_f c_f(\omega) \in [0,1].$$

This grows with the availability of important attributes and is always bounded in $[0,1]$.
Model disagreement κ. With three detectors, define the variance

$$\mathrm{Var}(\omega) = \frac{1}{3}\sum_{j=1}^{3} \left(s_j(\omega) - \bar{s}(\omega)\right)^2, \bar{s}(\omega) = s(\omega),$$

and normalize it to $[0,1]$ by

$$\kappa(\omega) = \min(1, 4\mathrm{Var}(\omega))$$

The factor 4 is tight because detector scores are in $[0,1]$ and the maximum variance is 0.25.
Neutrosophic triple (t, i, f). Map each event to support, indeterminacy, and conflict by

$$t(\omega) = q(\omega) \cdot 2\max(0, s(\omega) - 0.5), f(\omega) = q(\omega) \cdot 2\max(0, 0.5 - s(\omega)),$$
$$i(\omega) = \min\left(1, (1 - q(\omega)) + \frac{1}{2}\kappa(\omega)\right).$$

These formulas guarantee $t, i, f \in [0,1]$ for every event; t increases with confident pro-malicious evidence, f increases with confident pro-benign evidence, and i increases when features are missing or detectors disagree. Worked batch (six events). Use $\tau = 0.60$. For each event, the triple and the decision are computed exactly once; numbers are rounded to four decimals at the end.

ω_1 (malicious): detector scores $(0.88, 0.82, 0.90) \Rightarrow s = 0.8667$. Feature flags $(1,1,1) \Rightarrow q = 1.0$. Variance $= 0.0011556 \Rightarrow \kappa = 0.0046222$. Hence $t = 1.0 \times 2 \times (0.8667 - 0.5) = 0.7333$, $f = 0, i = (1 - 1) + 0.5 \times 0.0046222 = 0.0023$. Since $s \geq 0.60$, the prediction is malicious (TP).

ω_2 (malicious): detector scores $(0.70, 0.62, 0.63) \Rightarrow s = 0.6500$. Feature flags $(1,0,1) \Rightarrow q = 0.7$. Variance $= 0.0012667 \Rightarrow \kappa = 0.0050667$. Hence $t = 0.7 \times 2 \times (0.65 - 0.5) = 0.2100, f = 0$, $i = (1 - 0.7) + 0.5 \times 0.0050667 = 0.3025$. With $s \geq 0.60$, this is malicious (TP).

ω_3 (malicious): detector scores $(0.45, 0.52, 0.43) \Rightarrow s = 0.4667$. Feature flags $(1,1,0) \Rightarrow q = 0.8$. Variance $= 0.0014889 \Rightarrow \kappa = 0.0059556$. Hence $t = 0, f = 0.8 \times 2 \times (0.5 - 0.4667) = 0.0533, i = (1 - 0.8) + 0.5 \times 0.0059556 = 0.2030$. With $s < 0.60$, this is benign, but the truth is malicious (FN).

ω_4 (benign): detector scores $(0.78, 0.66, 0.72) \Rightarrow s = 0.7200$. Feature flags $(0,1,0) \Rightarrow q = 0.3$. Variance $= 0.0024000 \Rightarrow \kappa = 0.0096000$. Hence $t = 0.3 \times 2 \times (0.72 - 0.5) = 0.1320, f = 0$, $i = (1 - 0.3) + 0.5 \times 0.0096 = 0.7048$. With $s \geq 0.60$, this is malicious but the truth is benign (FP).

ω_5 (benign): detector scores $(0.58,0.52,0.55) \Rightarrow s = 0.5500$. Feature flags $(1,0,0) \Rightarrow q = 0.5$. Variance $= 0.0006000 \Rightarrow \kappa = 0.0024000$. Hence $t = 0.5 \times 2 \times (0.55 - 0.5) = 0.0500, f = 0$, $i = (1 - 0.5) + 0.5 \times 0.0024 = 0.5012$. With $s < 0.60$, this is benign (TN).

ω_6 (benign): detector scores $(0.12,0.18,0.20) \Rightarrow s = 0.1667$. Feature flags $(1,1,1) \Rightarrow q = 1.0$. Variance $= 0.0011556 \Rightarrow \kappa = 0.0046222$. Hence $t = 0, f = 1.0 \times 2 \times (0.5 - 0.1667) = 0.6667, i = (1 - 1) + 0.5 \times 0.0046222 = 0.0023$. With $s < 0.60$, this is benign (TN).

Confusion totals and deterministic metrics.

Counts are $\mathrm{TP} = 2(\omega_1, \omega_2), \mathrm{FP} = 1(\omega_4), \mathrm{FN} = 1(\omega_3), \mathrm{TN} = 2(\omega_5, \omega_6)$. Classical precision $= 2/(2 + 1) = 0.6667$, recall $= 2/(2 + 1) = 0.6667$, and $F_1 = 0.6667$. Deterministic error $\mathcal{R}_{\mathrm{det}} = (\mathrm{FP} + \mathrm{FN})/6 = 0.3333$.

Neutrosophic aggregation by cell. Sum the triples inside each cell:

TP totals: $t(\mathrm{TP}) = 0.7333 + 0.2100 = 0.9433, i(\mathrm{TP}) = 0.0023 + 0.3025 = 0.3048,$ $f(\mathrm{TP}) = 0$.

FP totals: $t(\mathrm{FP}) = 0.1320, i(\mathrm{FP}) = 0.7048, f(\mathrm{FP}) = 0$.

FN totals: $t(\mathrm{FN}) = 0, i(\mathrm{FN}) = 0.2030, f(\mathrm{FN}) = 0.0533$.

TN totals: $t(\mathrm{TN}) = 0.0500, i(\mathrm{TN}) = 0.5012, f(\mathrm{TN}) = 0.6667$.

Global sums over the batch are $T = \sum\ t = 0.9433 + 0.1320 + 0 + 0.0500 = 1.1253, I = \sum\ i = 0.3048 + 0.7048 + 0.2030 + 0.5012 = 1.7161$, and $F = \sum\ f = 0 + 0 + 0.0533 + 0.6667 = 0.7200$.

Neutrosophic performance. Using supportive masses only,

$$P_N = \frac{t(\mathrm{TP})}{t(\mathrm{TP}) + t(\mathrm{FP})} = \frac{0.9433}{0.9433 + 0.1320} = \frac{0.9433}{1.0753} = 0.8772 \text{ (rounded)}$$

$$R_N = \frac{t(\mathrm{TP})}{t(\mathrm{TP}) + t(\mathrm{FN})} = \frac{0.9433}{0.9433 + 0} = 1.0000$$

To price uncertainty on predicted positives, first compute $i(\mathrm{PredPos}) = i(\mathrm{TP}) + i(\mathrm{FP}) = 0.3048 + 0.7048 = 1.0096$ and $f(\text{ PredPos }) = 0$. With $\gamma = \delta = 0.5$,

$$P_N^{(0.5,0.5)} = \frac{0.9433}{0.9433 + 0.1320 + 0.5 \times 1.0096} = \frac{0.9433}{1.5801} = 0.5970(\text{ rounded }).$$

This quantity is monotone in the "bad" masses: decreasing i (PredPos) or f (PredPos) strictly increases $P_N^{(\gamma,\delta)}$ whenever $\gamma > 0$ or $\delta > 0$.

Budgeted neutrosophic risk. With nonnegative cost coefficients α, β, track

$$\mathcal{R}_N = \mathcal{R}_{\mathrm{det}} + \frac{\alpha I + \beta F}{6}$$

Choosing $\alpha = \beta = 0.25$ gives

$$\mathcal{R}_N = 0.3333 + \frac{0.25(1.7161 + 0.7200)}{6} = 0.3333 + \frac{0.609025}{6} = 0.3333 + 0.101504$$
$$= 0.4348 \text{ (rounded)}.$$

This is a single number that cleanly decouples deterministic mistakes from the explicit price of uncertainty and conflict. Actionable levers with guaranteed direction of improvement. Suppose an enrichment action clarifies a portion of the predicted-malicious set (for example, late sandbox verdicts), shifting Δi from indeterminacy to supportive mass on TP while keeping counts fixed. A 20% reduction of i (PredPos) yields $\Delta i = 0.20 \times 1.0096 = 0.2019$. Update $t(\text{TP}) \leftarrow 0.9433 + 0.2019 = 1.1452, i(\text{ PredPos }) \leftarrow 1.0096 - 0.2019 = 0.8077$, and the global $I \leftarrow 1.7161 - 0.2019 = 1.5142$. The penalized precision improves to

$$P_{N,\text{ ncw}}^{(0.5,0.5)} = \frac{1.1452}{1.1452 + 0.1320 + 0.5 \times 0.8077} = \frac{1.1452}{1.6811} = 0.6817(\text{ rounded }),$$

and the budgeted risk tightens to

$$\mathcal{R}_{N,\text{ new}} = 0.3333 + \frac{0.25(1.5142 + 0.7200)}{6} = 0.3333 + \frac{0.5586}{6} = 0.3333 + 0.0931$$
$$= 0.4264 \text{ (rounded)}.$$

Both directions are guaranteed by the algebra: decreasing $i(\text{ PredPos })$ cannot hurt $P_N^{(\gamma,\delta)}$ for $\gamma > 0$, and decreasing the global masses I or F cannot increase $\mathcal{R}_N$ for $\alpha, \beta \geq 0$.

6. Discussion and Practical Implications

The core contribution is an evaluation lens that keeps three facets of evidence-support t, indeterminacy i, and conflict f-throughout the pipeline. Instead of collapsing detector outputs into a single probability, the framework aggregates these masses over decision regions and reports neutrosophic precision and recall using only the supportive part, then adds a penalized precision that explicitly taxes ambiguity and counterevidence. A simple risk expression separates classical mistakes from the price of uncertainty, so changes in data quality or model calibration translate directly into measurable gains or costs.

The case study demonstrates this behavior with concrete numbers. On 1,000 emails at threshold $\tau = 0.60$, the system produces $\text{TP} = 270, \text{FP} = 70, \text{FN} = 30, \text{TN} = 630$, and a deterministic error of 0.1000. Aggregating the triples yields $t(\text{TP}) = 132.30$ and $t(\text{FP}) = 21.00$, which lifts neutrosophic precision to $P_N = 0.8630$ and recall to $R_N = 1.0000$, revealing strong supportive mass behind the true positives. Because predicted positives still carry uncertainty $i(\text{ PredPos }) = 118.50$, the penalized precision with $\gamma = \delta = 0.5$ is 0.6224 . The budgeted risk combines counts with global masses $I = 278.00$ and $F = 269.40$ to give an upper bound of 0.2369, which is the operational number to watch when uncertainty matters.

A realistic enrichment that converts 20% of i (PredPos) into supportive mass increases t (TP) to 156.00, reduces i (PredPos) to 94.80, and lowers the global indeterminacy to $I = 254.30$. Without touching the integer counts, the penalized precision rises to 0.6952 and the risk bound tightens to 0.2309. These monotone improvements follow directly from the formulas: reducing i or f can only

help the penalized precision and can only shrink the risk term when the penalty coefficients are nonnegative.

The interpretation is straightforward. High t on true positives indicates reliable support even when raw counts seem modest; large i on predicted positives flags missing or late features that should be prioritized for enrichment; elevated f in false positives points to over-reactive rules or miscalibrated detectors that require auditing. Because every quantity is bounded and every denominator is controlled, the metrics are stable in dashboards and safe in streaming computation. The framework, therefore, functions as a control system: it pinpoints where uncertainty lives, quantifies how much it costs, and predicts the benefit of specific actions before they are deployed.

7. Conclusion

This paper delivers a compact, deployable method for cybersecurity evaluation that preserves uncertainty instead of hiding it. The proposed evidence triplet, its integral-based aggregation, and the resulting metrics form a coherent control layer: they identify where ambiguity originates, quantify its operational cost, and indicate how specific interventions will improve outcomes. The procedure is deterministic, bounded, and parallelizable, so it fits high-throughput pipelines without numerical edge cases. Most importantly, it converts routine engineering action feature enrichment, detector calibration, and rule audits into predictable gains measured on the same scale as the evaluation itself. As a result, the framework is not only mathematically sound but also practically governing: teams can set targets, enact changes, and verify improvement using a single, consistent lens.

References

[1] Smarandache, F. (2013). Introduction to Neutrosophic Measure and Integral. arXiv preprint arXiv:1311.7139.

[2] Smarandache, F. (2015). Neutrosophic Precalculus and Neutrosophic Calculus. arXiv preprint arXiv:1509.07723.

[3] Alqahtani, H., Alsulami, A. A., Alsini, R., Alshammari, S., & Jahanshahi, H. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. Journal of Big Data, 11(1), 107. https://doi.org/10.1186/s40537-024-00957-y

[4] Agrawal, A., Dwivedi, R. K., & Hussain, M. (2022). Interval neutrosophic matrix game-based approach to counter cybersecurity issue in neutrosophic environment. Granular Computing, 7(4), 905-927. https://doi.org/10.1007/s41066-022-00327-0

[5] Sujatha, R., Bharathi, K. S., Jeyakumar, M. K., Preethi, S., & Tamilarasi, K. (2024). Modelling attack and defense games in infrastructure networks with interval-valued intuitionistic fuzzy graphs. Complex & Intelligent Systems, 10(4), 1-16. https://doi.org/10.1007/s40747-024-01495-z

[6] Yadav, S. P. (2024). A Multi-Criteria Decision-Making Framework to Evaluate the Impact of Industry 4.0 Technologies on Sustainability Using Neutrosophic AHP. Information Systems Frontiers, 26(3), 1-19. https://doi.org/10.1007/s10796-024-10472-3

[7] Ferrag, M. A., & Shu, L. (2025). Artificial intelligence and machine learning in cybersecurity: A comprehensive survey of intrusion detection, challenges, and prospects. Knowledge and Information Systems, 67(5), 1-38. https://doi.org/10.1007/s10115-025-02429-y

[8] Abdel-Basset, M., Mohamed, R., & Sallam, K. (2025). A Multi-criteria Framework for Supplier Assessment Based on Neutrosophic Sets and CODAS Method. International Journal of Fuzzy Systems, 27(4), 1-17. https://doi.org/10.1007/s40815-025-02066-1

[9] Balaji, P. G., Srinivasan, S., Suganya, P. D., & Suresh, D. (2025). A comprehensive review of generative AI techniques and their applications in cybersecurity. Soft Computing, 29(12), 1-20. https://doi.org/10.1007/s00500-025-10702-z

[10] Abdel-Basset, M., Mohamed, R., Elhoseny, M., & Chang, V. (2025). AI software selection for cybersecurity auditing using neutrosophic CRITIC-CODAS method. Applied Soft Computing, 164, 112165. https://doi.org/10.1016/j.asoc.2025.112165

[11] Mahajan, V. (2025). Leveraging AI for enhanced cybersecurity: a comprehensive review. SN Applied Sciences, 7(6), 345. https://doi.org/10.1007/s42452-025-06773-0

[12] Sarker, I. H. (2025). Generative AI revolution in cybersecurity: a comprehensive review of threats, risks, and solutions. Artificial Intelligence Review, 58(5), 1-40. https://doi.org/10.1007/s10462-025-11219-5

[13] Salama, A. A., Elsafty, M., & Elsayad, M. (2025). Machine Learning Models with Neutrosophic Numbers for Cloud Security Threats. Neutrosophic Systems with Applications, 18, 1-12. https://doi.org/10.61356/j.nswa.2025.183383

[14] Alshammari, S. (2024). A neutrosophic framework for evaluating security measures in cloud computing services. Journal of Fuzzy Extension and Applications, 5(2), 1-15.

[15] Abdel-Basset, M., Mohamed, R., & Elzein, I. (2023). Neutrosophic MCDM Methodology for Assessment Risks of Cyber Security in Power Management. Neutrosophic Systems with Applications, 9, 30-46. https://doi.org/10.61356/j.nswa.2023.11

[16] Ferrag, M. A., Shu, L., & Djallel, H. (2025). Emerging AI threats in cybercrime: a review of zero-day attacks via machine learning. Knowledge and Information Systems, 67(9), 1-27. https://doi.org/10.1007/s10115-025-02556-6

[17] Al-Gethami, H. M., Al-Ghamdi, M. S., & Ragab, M. (2022). Violence Detection Approach based on Cloud Data and Neutrosophic Cognitive Maps. Journal of Cloud Computing: Advances, Systems and Applications, 11(1), 85. https://doi.org/10.1186/s13677-022-00369-4

[18] Buczak, A. L., & Guven, E. (2024). The role of AI in cybersecurity: Trends and applications. Journal of Cybersecurity Education, Research and Practice, 2024(1), 1-15.

[19] Sarker, I. H. (2024). AI-driven cybersecurity: An overview, security intelligence modeling and research directions. SN Computer Science, 2(3), 173.

[20] Talukder, M. A., Hasan, K. F., & Ahmed, M. (2025). AI, machine learning and deep learning in cyber risk management. Digital Finance, 7(2), 1-20. https://doi.org/10.1007/s43621-025-01012-3

[21] Truică, C. O., & Paschke, A. (2025). Artificial intelligence and machine learning in cybersecurity. Knowledge and Information Systems, 67(4), 1-35.

[22] Koch, S., Schneider, S., & Plattner, B. (2025). An iterative five-phase process model to successfully implement AI for cybersecurity. Electronic Markets, 35(1), 1-20. https://doi.org/10.1007/s12525-025-00802-x

[23] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2021). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. Complex & Intelligent Systems, 7(2), 897-920. https://doi.org/10.1007/s40747-021-00494-8

[24] Terzi, D. S., Terzi, R., & Sagiroglu, S. (2024). Artificial intelligence for system security assurance: A systematic literature review. International Journal of Information Security, 23(3), 1-25. https://doi.org/10.1007/s10207-024-00959-0

[25] Sharma, S., Gupta, S., & Singh, R. (2025). Design and Computational Modeling of an AI-Based Automated Cybersecurity System. IEEE Transactions on Computational Social Systems, 12(4), 1500-1510. https://doi.org/10.1109/TCSS.2025.11145017

Received: April 26, 2025. Accepted: Aug 31, 2025