Enhancing Business Cybersecurity Through Integrated Defense and Incident Response: A Comparative Decision Framework

Aligned with NIST CSF 2.0, NIST SP 800-61r3, ISO/IEC 27001: 2022, CIS Controls v8.1, and MITRE ATT&CK

Jurgen Mecaj
Department of Information Technology (DTI)-Faculty of Informatics, Mediterranean University of Albania, Tirana, Albania

***Abstract*—Business operations increasingly depend on digital workflows, hybrid infrastructures, and third-party ecosystems, making cybersecurity incidents a direct business continuity and governance problem rather than solely a technical concern. This paper proposes an integrated cyber defense and defense-to-response decision framework for organizations seeking to reduce exposure to external attacks and unauthorized access while improving incident detection, containment, and recovery. The framework aligns governance and control selection with NIST Cybersecurity Framework (CSF) 2.0, operational incident response considerations with NIST SP 800-61 Revision 3, control requirements with ISO/IEC 27001:2022, prioritized safeguards with CIS Controls v8.1, and adversary-behavior mapping with the MITRE ATT&CK Enterprise Matrix. We define an evaluation model that combines 1) coverage mapping across prevent-detect-respond-recover functions, 2) multi-criteria decision analysis (MCDA) for cost, complexity, and risk reduction trade-offs, and 3) a playbook-oriented response design for high-frequency attack paths relevant to business environments. A worked comparative example demonstrates how three strategy bundles (traditional perimeter controls, defense-in-depth with SIEM, and a Zero Trust + EDR + SOAR approach) can be ranked using weighted criteria and incident lifecycle metrics. The paper concludes with an implementation roadmap and measurement plan to convert the framework into an evidence-based program that supports executive decision-making and continuous improvement.**

Keywords*—Cyber defense; incident response; business continuity; NIST CSF 2.0; SP 800-61r3; ISO/IEC 27001:2022; CIS Controls v8.1; MITRE ATT&CK; Zero Trust; EDR; SOAR; MCDA

I. Introduction

For most organizations, cybersecurity risk has matured into a business risk: incidents can halt operations, drive regulatory exposure, damage trust, and increase cost of capital. Recent industry analyses continue to report large volumes of real-world incidents and breaches, reinforcing the need for defense strategies tightly coupled with rapid response and recovery. In parallel, adversaries increasingly use credential theft, infostealers, and exploitation of weak security hygiene during cloud and hybrid transitions, elevating the probability of unauthorized access and lateral movement in business networks. Recent industry reports highlight persistent breach drivers and the business impact of incident response performance [6]–[8].

Despite substantial investment in security tooling, many organizations struggle to convert controls into measurable improvements in mean time to detect (MTTD), mean time to respond (MTTR), and overall business resilience. Common failure modes include fragmented governance, inconsistent prioritization, limited logging visibility, and response playbooks that are not exercised or automated.

This research addresses the doctoral theme of increasing cybersecurity as a practical instrument for protecting business activity from external attacks and unauthorized access by proposing a comparative, standards-aligned decision framework that connects: 1) cybersecurity governance and prioritization, 2) defensive control bundles, 3) ATT&CK-informed detection logic, and 4) incident response execution and recovery.

Novelty and positioning: Unlike catalog-only maturity views, the proposed approach formalizes defense-to-response strategy bundles as the decision unit and jointly evaluates standards-aligned controls, ATT&CK-informed coverage evidence, and incident lifecycle/continuity signals (e.g., MTTD, MTTR, containment and restoration outcomes). This coupling supports explicit trade-off analysis across prevention, detection, response automation, and recovery under realistic constraints.

The remainder of this paper is organized as follows: Section I states the research objectives and contributions. Background and related guidance are presented in Section II. Section III presents the methodology. Section IV presents the worked comparative example. Section V details standards mapping and comparison. Section VI provides incident response for playbook matrix. Section VII presents roadmap for businesses. Section VIII discusses implementation considerations and limitations, and Section IX concludes with future research directions.

A. Research Objectives and Questions

The primary objective is to provide a repeatable method for selecting and validating defense and incident response

strategies that measurably improve business protection. The paper is guided by the following research questions (RQs):

RQ1: Which defense-to-response strategy bundles provide the best balance between risk reduction and operational feasibility for business environments?

RQ2: How can organizations compare strategy bundles using a transparent scoring model aligned with recognized standards and adversary behaviors?

A conceptual decision lens that links governance, control selection, telemetry, and incident execution into a single evaluable strategy bundle aligned with recognized standards.

A comparative evaluation model combining ATT&CK coverage validation with MCDA-based scoring tied to operational detection/response and recovery indicators.

- A playbook matrix that operationalizes frequent business-relevant attack paths into detection, containment, and recovery actions to support repeatability and continuous improvement.
- A measurement and roadmap approach describing how organizations calibrate criteria and weights using exercises and incident data to generalize beyond the illustrative example.
- A practical playbook matrix for frequent business-relevant attack paths, supporting repeatable response and continuous improvement.
- A measurement plan linking technical outcomes to business continuity indicators.

II. Background and Related Guidance

NIST SP 800-61r3 provides practical incident response guidance, including preparation, detection/analysis, containment/eradication/recovery, and post-incident improvement, aligned with CSF 2.0 risk management needs [2].

NIST CSF 2.0 provides a taxonomy for governance, risk prioritization, and continuous improvement across the cybersecurity lifecycle [1].

[2] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," NIST Special Publication 800-61r3, Apr. 2025. doi:10.6028/NIST.SP.800-61r3.

ISO/IEC 27001:2022 defines requirements for an information security management system (ISMS) and establishes a compliance-oriented control portfolio [3].

In addition, NIST SP 800-53 Rev. 5 provides a detailed control catalog and baselines that can be mapped to organizational requirements and evidence collection activities [9].

Risk assessment approaches such as NIST SP 800-30r1 support structured identification and analysis of threats, vulnerabilities, and likelihood/impact, informing prioritization of control bundles and response investments [10].

ISO/IEC 27005:2022 extends ISO/IEC 27001 programs with information security risk management guidance across assessment, treatment, monitoring, and communication, reinforcing a continuous improvement cycle [11].

Quantitative methods such as the Open FAIR approach complement qualitative scoring by estimating loss event frequency and magnitude, enabling financial risk communication and investment justification [12].

For criteria weight elicitation, analytic hierarchy process (AHP) is a widely used structured technique for pairwise comparison of decision criteria and can be applied to reduce subjective bias in stakeholder weighting workshops [13].

These perspectives motivate an integrated decision approach that connects standards compliance, threat-informed coverage, and operational incident outcomes rather than treating them as independent workstreams.

CIS Controls v8.1 provides a prioritized set of safeguards and introduces governance recommendations aligned with modern environments [4].

MITRE ATT&CK provides a behavior-based model of adversary tactics and techniques used to design detections and validate coverage [5].

A. Integrated Reference Architecture

Fig. 1 summarizes a practical defense-to-response reference architecture that connects monitoring, analysis, orchestration, containment, and governance. The architecture supports both preventive hardening and post-incident learning loops.

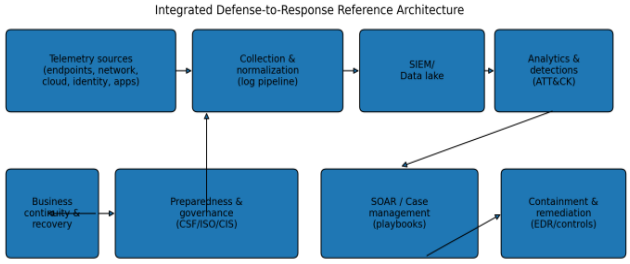

Fig. 1. Integrated defense-to-response reference architecture (conceptual).

III. Methodology

The proposed methodology combines 1) threat-informed defense mapping, 2) a multi-criteria decision analysis (MCDA) scoring model, and 3) playbook-driven incident response design. The methodology is intended to be executed iteratively and improved with measurement data.

A. Strategy Bundles

Organizations typically deploy controls as tool-by-tool procurements; however, business protection depends on coherent bundles that span identity, endpoint, network, logging, and recovery. We define three common strategy bundles used for comparison:

S1: Traditional (perimeter + antivirus + basic backups): Emphasizes perimeter defenses and endpoint antivirus with limited centralized visibility and manual response.

S2: Defense-in-depth (MFA + vulnerability management + segmentation + SIEM): Adds identity hardening and centralized logging/analytics to improve detection and investigation.

Note on criterion interactions: The weighted-sum model is simplest and transparent, but it assumes limited interaction among criteria. In practice, detection coverage and response speed may be positively coupled via improved telemetry and triage. To mitigate interaction risk, organizations should document dependencies, perform sensitivity analysis over weights, and, where needed, use interaction-aware extensions (e.g., ANP or multi-objective formulations) when dependencies materially affect ranking.

S3: Zero Trust + EDR/XDR + SIEM + SOAR + PAM + immutable backups: Implements strong identity controls, behavior-based detection, automated response, and resilient recovery capabilities.

B. Evaluation Criteria and Weighting

To compare strategy bundles transparently, we define eight criteria spanning prevention, detection, response, recovery, and feasibility. Weights can be determined via stakeholder workshops or analytic hierarchy process (AHP). For the worked example, we use the weights in Table I.

TABLE I. EVALUATION CRITERIA AND EXAMPLE WEIGHTS FOR MCDA SCORING

Criterion	Definition (business-oriented)	Weight
Attack surface reduction	Hardening and exposure reduction (patching, segmentation, secure configuration, asset control).	0.15
Identity & access hardening	MFA, least privilege, PAM, and identity monitoring to reduce unauthorized access.	0.15
Detection coverage & fidelity	Visibility and detection quality across endpoints, network, cloud, and identity.	0.18
Response speed & orchestration	Case management, automation, containment capability, and repeatable playbooks.	0.18
Resilience & recovery	Backups, restoration confidence, disaster recovery, and continuity of critical services.	0.12
Governance & compliance support	Support for CSF/ISO control evidence, policies, risk reporting, and audits.	0.10
Cost (lower is better)	Total cost of ownership relative to risk reduction (higher score = lower cost).	0.07
Operational complexity (lower is better)	Staffing and operational burden (higher score = easier operation).	0.05

C. Scoring Model

Each strategy bundle is scored on a 1-5 ordinal scale per criterion, where higher values indicate better performance (except that cost and complexity are inverted so higher values represent lower cost/complexity). Scores are normalized to [0,1] and aggregated using a weighted sum model:

$$\text{Score(bundle)} = \Sigma\_i \, w\_i \times (s\_i / 5)$$

D. Threat-Informed Coverage Mapping

To avoid purely subjective scoring, organizations should map control bundles to a threat model based on business context (industry, assets, and common attack paths) and validate with ATT&CK techniques. Detection engineering should explicitly document which ATT&CK techniques are covered by telemetry, analytics, and response actions.

E. Measurement Plan

A measurement plan converts the framework into an evidence-based program. Recommended operational metrics include:

- Mean time to detect (MTTD) and mean time to respond. (MTTR)
- Containment success rate within defined service-level objectives (SLOs).
- Restoration time and data integrity confidence for critical systems.
- Detection false positive rate and analyst workload Fig. 2 helps identify which criteria drive strengths and weaknesses, while Fig. 3 summarizes the overall ranking implied by the chosen weights, supporting executive-level comparison.
- Coverage maturity: percentage of prioritized ATT&CK techniques with validated detections and tested playbooks.
- Business impact: downtime, recovery cost, regulatory notifications, and customer-facing disruption.

IV. WORKED COMPARATIVE EXAMPLE (ILLUSTRATIVE)

This section provides a worked example using illustrative values to demonstrate how the framework operates. Organizations should calibrate the example scores and weights using internal measurements, controlled exercises, and operational incident data prior to deployment.

A. Comparative Scoring Matrix

Table II reports the illustrative 1–5 criterion scores assigned to each strategy bundle; these values are used to normalize and aggregate the MCDA composite ranking.

TABLE II. ILLUSTRATIVE 1-5 SCORING FOR STRATEGY BUNDLES ACROSS EVALUATION CRITERIA

Criterion (1-5)	S1 Traditional (perimeter+AV)	S2 Defense-in-depth (MFA+SIEM)	S3 Zero Trust + EDR + SOAR
Attack surface reduction	2	4	5
Identity & access hardening	2	4	5
Detection coverage & fidelity	2	3	5
Response speed & orchestration	1	3	5
Resilience & recovery	3	4	5
Governance & compliance	2	4	5
Cost (lower is better)	5	3	2
Ops complexity (lower is better)	4	3	2

These indicators can be operationalized through incident tickets and post-incident reviews to validate whether improvements translate into reduced downtime and faster recovery.

B. Visualization

Fig. 2 presents the comparative profile across criteria, while Fig. 3 shows the aggregated weighted composite score.

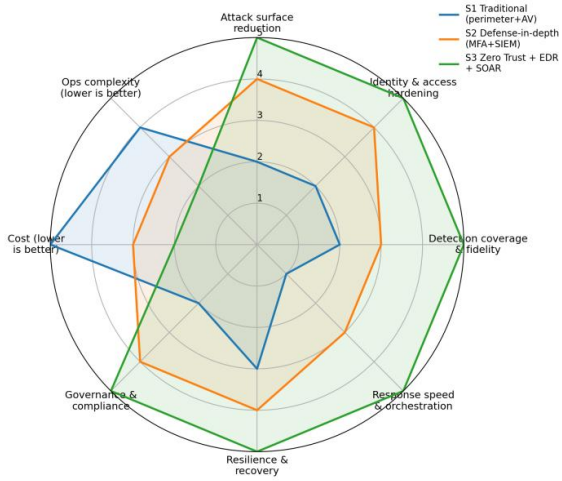

Fig. 2. Radar plot of comparative criterion scores (illustrative).

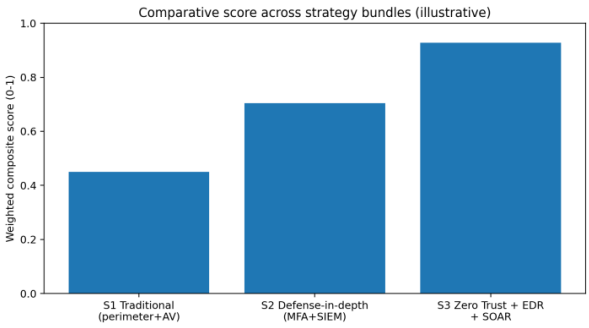

Fig. 3. Weighted composite score across strategy bundles (illustrative).

C. Incident Lifecycle Improvement Indicators

Beyond composite scoring, executive stakeholders typically require operational indicators that translate to reduced disruption. Fig. 4 illustrates how stronger detection and response capabilities can reduce MTTD/MTTR, improving containment and recovery speed.

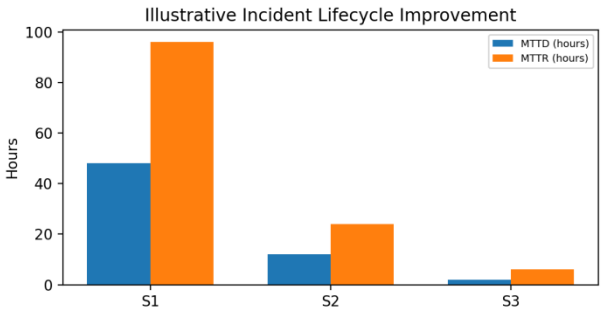

Fig. 4. Illustrative MTTD and MTTR comparison.

D. Interpretation of the Worked Example

Using the example weights, S3 (Zero Trust + EDR + SOAR) achieves the highest composite score primarily due to strong detection coverage, orchestration, and recovery. S2 provides a cost-balanced intermediate option with material gains over S1. However, organizational constraints (budget, staffing, regulatory priorities, legacy systems) may justify selecting S2 as a transition architecture with an incremental roadmap toward S3.

V. Standards Mapping and Comparison

Table III provides a high-level conceptual mapping between program activities and the referenced standards/guidance, supporting traceability from governance to incident handling and recovery.

A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," NIST Special Publication 800-61r3, Apr. 2025. doi:10.6028/NIST.SP.800-61r3 [2].

TABLE III. High-Level Mapping Across Standards and Guidance (Conceptual)

Program activity	NIST CSF 2.0	NIST SP 800-61r3	ISO/IEC 27001:2022	CIS Controls v8.1
Governance & policy	Govern	Govern/Prepare (CSF-aligned IR considerations)	ISMS context, leadership, planning	Governance function (v8.1)
Asset & exposure management	Identify, Protect	Preparation considerations	Operational planning, controls selection	Inventory, vulnerability management
Detection engineering	Detect	Detection/analysis considerations	Monitoring controls (Annex A - technological)	Audit log management, monitoring
Incident handling	Respond	Incident response recommendations	Incident management controls, continuous improvement	Incident response management
Recovery & resilience	Recover	Recovery considerations	Business continuity and backup controls	Data protection, recovery safeguards
Continuous improvement	Govern (improve), all functions	Lessons learned integration	Internal audit, management review, improvement	Metrics and program improvement

A. Why Behavior-Based Mapping Matters

Control catalogs alone do not ensure coverage against real attacker tradecraft. ATT&CK-based mapping helps validate whether telemetry and analytics cover the tactics most relevant to unauthorized access (Initial Access, Credential Access, Lateral Movement, Privilege Escalation, Exfiltration) and whether response actions can disrupt those tactics within required SLOs.

VI. Incident Response Playbook Matrix

Table IV provides a compact playbook matrix for business-relevant scenarios. Each scenario should be backed by detailed procedures, communications templates, legal/regulatory triggers, and evidence handling guidance.

TABLE IV. Playbook Matrix for High-Frequency Scenarios (Conceptual)

Scenario	Primary ATT&CK focus	Key detection signals	Containment actions	Recovery actions
Credential theft / infostealer-driven intrusion	Credential Access, Initial Access, Lateral Movement	Unusual auth patterns, token abuse, new device logins, anomalous process chains	Force MFA reset, revoke tokens/sessions, isolate affected endpoints, block IOCs	Password rotation, reimage endpoints, validate privileged accounts, review access logs
Ransomware attempt (pre-encryption)	Execution, Defense Evasion, Impact	Mass file modifications, suspicious scheduled tasks, EDR ransomware heuristics	Isolate hosts, disable SMB shares, block lateral movement, snapshot evidence	Restore from immutable backups, validate integrity, re-enable services with monitoring
Web application exploitation	Initial Access, Persistence, Exfiltration	WAF alerts, abnormal API patterns, new admin accounts, DB query anomalies	Disable vulnerable endpoints, rotate secrets, patch, activate emergency rules	Forensic review, restore clean images, rotate keys, customer notification if required
Business email compromise (BEC)	Initial Access, Credential Access, Collection	Mailbox forwarding rules, abnormal OAuth grants, finance workflow anomalies	Disable account, revoke OAuth grants, remove rules, hold suspicious transfers	Financial recovery steps, strengthen approvals, awareness reinforcement

VII. Implementation Roadmap for Businesses

A phased roadmap helps organizations transition from tool-centric security to a measurable defense-to-response program.

A. Phase 0 - Governance and Scope

Define critical business processes, crown-jewel assets, risk appetite, and reporting cadence. Establish a governance model aligned to CSF 2.0 and define incident categories, notification thresholds, and decision rights.

B. Phase 1 - Baseline Hygiene and Visibility

Implement asset inventory, vulnerability management, secure configuration baselines, and MFA for privileged access. Enable centralized logging for identity, endpoint, network, and cloud platforms. Confirm backup integrity and restoration procedures for critical systems.

C. Phase 2 - Threat-Informed Detections and Exercises

Develop prioritized detection use cases mapped to ATT&CK techniques relevant to the business. Conduct tabletop exercises and controlled attack emulation to validate detection and response. Measure MTTD/MTTR and refine playbooks.

D. Phase 3 - Orchestration, Automation, and Resilience

Introduce SOAR for routine containment steps, ticketing integration, and standardized communications. Adopt Zero Trust principles and privileged access management where feasible. Strengthen recovery with immutable backups and tested disaster recovery runbooks.

VIII. Discussion and Limitations

The proposed framework is designed to be practical and auditable; however, it does not replace empirical evaluation. Scoring models can introduce bias if weights and criteria are not validated by stakeholders and measured outcomes. Additionally, organizations with constrained resources may prioritize incremental adoption (S2) as a stepwise path toward a higher maturity state (S3). Future empirical work should validate the model with measured incident datasets, controlled attack emulation, and longitudinal business impact analysis.

IX. Conclusion

Protecting business operations from external attacks and unauthorized access requires more than deploying isolated security tools; it requires a coherent defense-to-response program that links governance, detection engineering, and incident response execution. This paper presented a comparative, standards-aligned decision framework combining ATT&CK-informed mapping, MCDA scoring, and playbook-driven response design. The worked example illustrates how organizations can rank strategy bundles and communicate trade-offs to executives. By integrating measurement (MTTD/MTTR, containment success, recovery time, and coverage maturity), the framework enables continuous improvement and supports cybersecurity as a practical instrument for safeguarding business activity. The framework is intended to be applied iteratively as evidence accumulates through exercises and operational incidents.

Limitations include dependence on organizational context, scoring subjectivity, and incomplete observability for certain techniques; these can be reduced through exercises, purple-team validation, and periodic recalibration of weights and scores.

Future research should empirically validate rankings across diverse sectors, automate ATT&CK-to-detection-to-playbook evidence collection, and compare MCDA results with quantitative risk models (e.g., Open FAIR) and alternative decision methods under uncertainty.

References

[1] National Institute of Standards and Technology (NIST), The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, Feb. 26, 2024.

[2] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, "Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile," NIST Special Publication 800-61r3, Apr. 2025. doi:10.6028/NIST.SP.800-61r3.

[3] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27001:2022 Information

security, cybersecurity and privacy protection - Information security management systems - Requirements, 2022.

[4] Center for Internet Security (CIS), CIS Critical Security Controls v8.1, June 25, 2024.

[5] MITRE, MITRE ATT&CK Enterprise Matrix (online resource).

[6] Verizon, 2025 Data Breach Investigations Report (DBIR), 2025.

[7] IBM Security and Ponemon Institute, Cost of a Data Breach Report 2025, 2025.

[8] Google Cloud (Mandiant), M-Trends 2025 Report, 2025.

[9] NIST, Security and Privacy Controls for Information Systems and Organizations, NIST SP 800-53 Revision 5, 2020.

[10] NIST, Guide for Conducting Risk Assessments, NIST SP 800-30 Revision 1, Sept. 2012. doi:10.6028/NIST.SP.800-30r1.

[11] International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC), ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks, 2022.

[12] The Open Group, Open FAIR Risk Analysis Process Guide, The Open Group Guide (G180), Sept. 2022.

[13] R. W. Saaty, "The analytic hierarchy process-what it is and how it is used," Mathematical Modelling, vol. 9, no. 3-5, pp. 161-176, 1987. doi:10.1016/0270-0255(87)90473-8.