LARES

A DAMOVO COMPANY

LARES

BRIDGING TTX AND TTP EMULATION

THE 6-STEP ADVERSARIAL INTEGRATION METHODOLOGY

Stop guessing and start proving.

The 6-Step Adversarial Integration Methodology is your definitive guide to bridging executive tabletop exercises with live-fire TTP emulation. Discover how to eliminate the illusion of readiness, hold your security stack accountable, and transform assumption-based plans into a measurable, evidence-backed defense.

ABOUT LARES

Lares is an offensive security firm that helps companies secure electronic, physical, intellectual, and financial assets through a unique blend of assessment, testing, and coaching since 2008.

For more information, visit lares.com, contact us at (720) 600-0329, or email sales@lares.com

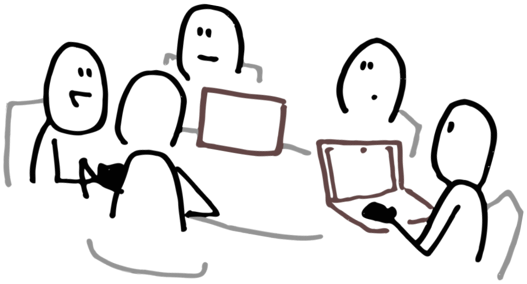
CONTACT INFORMATION

Eric Smith - Co-founder & Group CEO

+1 (720) 600-0329
sales@lares.com

https://www.lares.com

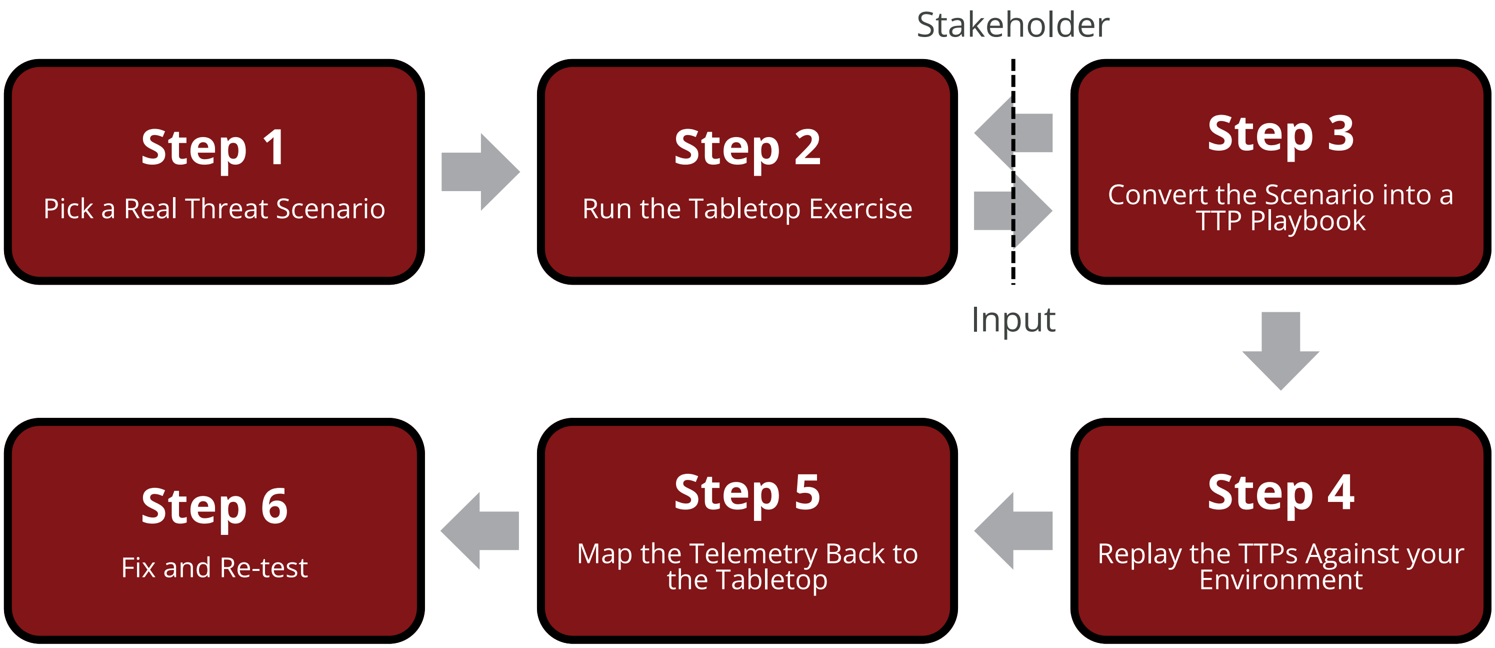
Executive Summary



The cybersecurity industry operates under a significant illusion of readiness. According to industry benchmarking, 94% of surveyed organizations confidently believe they can effectively detect, respond to, or recover from a major incident. However, when tested in realistic decision drills, teams achieve only a 22% decision accuracy rate. Furthermore, these teams typically require a median of 29 hours to contain simulated attacks. This readiness gap is real.

Traditional Tabletop Exercises (TTX) strip away the illusion of coordination by exposing breakdowns in communication, escalation paths, and decision bottlenecks under pressure. While a TTX functions as the "brain" of an organization by testing people, process, and policy , it fails to answer a critical technical question: did the security stack ever detect the attack in the first place? Conversely, Tactics, Techniques, and Procedures (TTP) replay acts as the "nervous system". It tests what technical controls actually do closer to the keyboard. Running a TTX alone improves plans, and running a TTP replay alone improves detections.

Running them together uncovers the truth. This 6-Step Adversarial Integration Methodology is a closed-cycle validation model designed to expose the cracks via TTX and verify the technical fixes via TTP replay. This methodology provides board-level risk committees with documented, repeatable proof of readiness rather than self-assessment theater.



Stakeholder

Step 1
Pick a Real Threat Scenario

Step 2
Run the Tabletop Exercise

Step 3
Convert the Scenario into a TTP Playbook

Input

Step 4
Replay the TTPs Against your Environment

Step 5
Map the Telemetry Back to the Tabletop

Step 6
Fix and Re-test

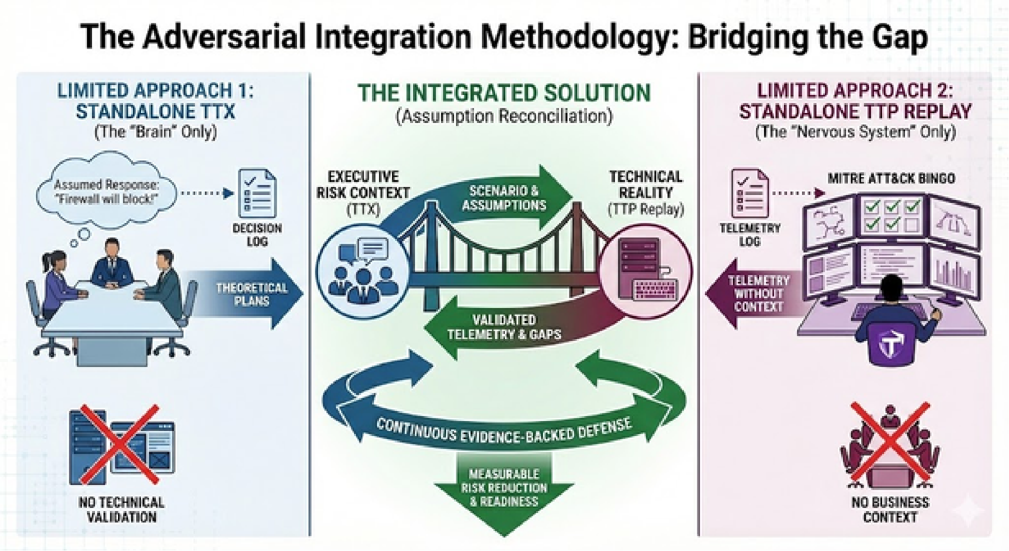
Theoretical and Strategic Foundations

The prevalent approach to security validation often relies on isolated testing methodologies. Standalone tabletop exercises rely heavily on notional artifacts and assumed technical responses. Participants frequently assume that a firewall will block an attack or that an Endpoint Detection and Response (EDR) tool will generate an alert, allowing the exercise to move on without technical verification.

Alternatively, compliance-driven testing and standalone purple teaming often fall victim to the pursuit of framework coverage. Security teams attempt to play "MITRE ATT&CK bingo" by testing as many techniques as possible, regardless of environmental relevance. This approach prioritizes control coverage over control effectiveness.

The Adversarial Integration Methodology introduces the concept of assumption reconciliation as a primary governance control. By taking the notional output and assumptions of a previous TTX engagement and replaying those specific behaviors in the environment, organizations measure the actual effectiveness of their technical controls.

Critics argue that Continuous Threat and Exposure Management (CTEM) or frequent purple teaming is sufficient for defensive maturity. However, without the business risk context and executive decision sequencing provided by a TTX, technical telemetry lacks operational prioritization. The integration of both exercises bridges the age-old chasm between technical threat and organizational risk.



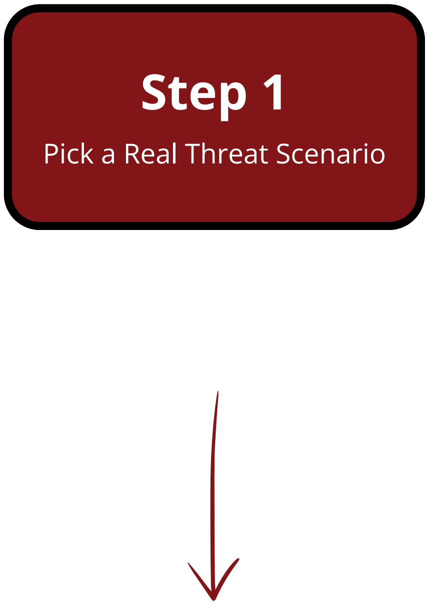
The Adversarial Integration Methodology: Bridging the Gap
LIMITED APPROACH 1: STANDALONE TTX
(The "Brain" Only)
Assumed Response: "Firewall will block!"
DECISION LOG
THEORETICAL PLANS
NO TECHNICAL VALIDATION
THE INTEGRATED SOLUTION
(Assumption Reconciliation)
EXECUTIVE RISK CONTEXT (TTX)
SCENARIO & ASSUMPTIONS
TECHNICAL REALITY (TTP Replay)
VALIDATED TELEMETRY & GAPS
CONTINUOUS EVIDENCE-BACKED DEFENSE
MEASURABLE RISK REDUCTION & READINESS
LIMITED APPROACH 2: STANDALONE TTP REPLAY
(The "Nervous System" Only)
TELEMETRY LOG
MITRE ATT&CK BINGO
TELEMETRY WITHOUT CONTEXT
NO BUSINESS CONTEXT

The 6-Step Adversarial Integration Methodology

Step 1: Threat-Informed Scenario Architecture

The methodology begins by selecting a highly relevant scenario that impacts the specific organization.

- **Data Synthesis:** Scenarios must be synthesized from internal Cyber Threat Intelligence (CTI), sector-specific information sharing and analysis centers (ISACs), and external threat blogs. Governance and legal stakeholders should also provide input regarding third-party risks affecting the business.
- **Believability:** If a scenario is not believable, exercise participants will check out early. Threat narratives must target specific business-unit critical processes, such as ransomware in a specific business unit or cloud identity misuse.



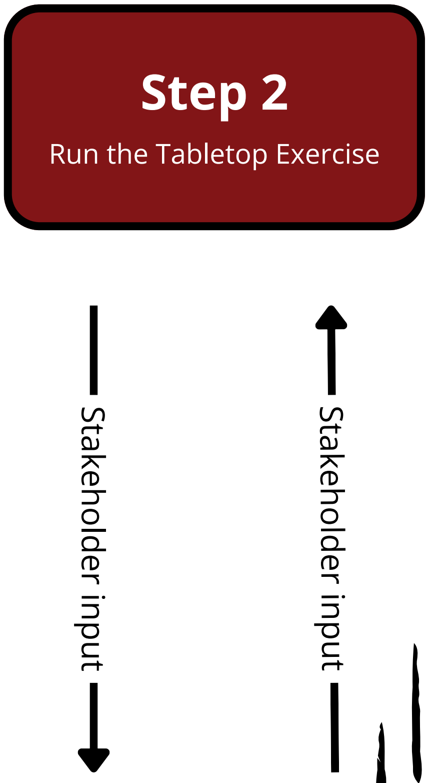
Step 1

Pick a Real Threat Scenario

Step 2: Execution of the Process and Policy Tabletop (TTX)

The TTX phase operates as an organizational stress simulation.

- **Execution Protocols:** The exercise must capture assumptions, decisions, process owners, and escalation paths. It exposes who freezes when decisions get messy and where regulatory reporting gets missed.
- **Assumption Auditing:** Facilitators must rigorously document technical assumptions. When participants state a firewall will block an action or an analyst will see a specific Security Information and Event Management (SIEM) alert, these statements become the baseline for the next step.
- **Regulatory Modeling:** The TTX must model strict timelines for containment and public communication, simulating the pressure of containing a narrative before an SEC 8-K must be reported.



Step 2

Run the Tabletop Exercise

Stakeholder input

Stakeholder input

Step 3: Adversarial Playbook Translation

Following the TTX, the captured assumptions are converted into a technical playbook for adversarial behavior.

- **TTP Definition:** The playbook must define exact attacker behaviors and techniques relevant to the environment based on the TTX.
- **Prioritization:** Instead of exhausting a framework taxonomy, engineering must prioritize specific attack vectors discussed in the TTX, including credential theft and reuse, living-off-the-land pivots, and data exfiltration through approved channels.
- **Stakeholder Input Loop:** The playbook development requires continuous feedback from stakeholders to ensure the technical execution aligns with the priorities of top-line management.

Step 3

Convert the Scenario into a TTP Playbook

Step 4: Live-Fire TTP Emulation (Purple Teaming)

The organization conducts a live purple team engagement to execute the engineered playbook in the production environment.

- **Execution:** Hands-on-keyboard execution of simulated or emulated attacks validates whether assumed behaviors actually happen in the environment.
- **Telemetry Collection:** Engineers must gather raw alert data, identify visibility gaps, and record response timing.
- **Measurement:** This step tracks the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) while analyzing layered architecture performance. It answers whether the SOC saw the activity, if logging existed where assumed, and if alerts fired from both the EDR and the SIEM.

Step 4

Replay the TTPs Against your Environment

Step 5: Telemetry and Assumption Reconciliation

This critical phase merges the outputs of the previous steps to quantify actual defensive capabilities.

- **Reconciliation Framework:** Telemetry gathered during the TTP replay is mapped directly back to the assumptions made during the TTX to expose detection gaps.
- **Vendor Accountability**: This step proves what products actually detect versus what vendors claim they detect. It validates the return on security investments (ROSI) by confirming technologies perform as intended.
- **Visibility Blind Spots:** It turns the phrase "we think we would catch that" into verifiable proof based on technical artifacts.

Step 5

Map the Telemetry Back to the Tabletop

Step 6: Remediation, Tuning, and Validation Retesting

The organization conducts a live purple team engagement to execute the engineered playbook in the production environment.

- **Execution:** Hands-on-keyboard execution of simulated or emulated attacks validates whether assumed behaviors actually happen in the environment.
- **Telemetry Collection:** Engineers must gather raw alert data, identify visibility gaps, and record response timing.
- **Measurement:** This step tracks the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) while analyzing layered architecture performance. It answers whether the SOC saw the activity, if logging existed where assumed, and if alerts fired from both the EDR and the SIEM.

Step 6

Fix and Re-test

Regulatory and Governance Alignment

Executive boards are actively requesting evidence that tabletop exercises are occurring at a regular cadence. They do not want raw technical data regarding remediated vulnerabilities; they require documented proof of readiness showing that organizational risks are kept at acceptable levels.

This methodology aligns directly with strict regulatory monitoring frameworks. By testing escalation timing and reporting protocols during the TTX, organizations prepare for rapid public disclosures, such as those mandated by the Securities and Exchange Commission (SEC). The subsequent TTP replay provides the empirical audit evidence required to support defensible disclosure narratives, shifting the compliance posture from assumed readiness to evidence-backed reality.

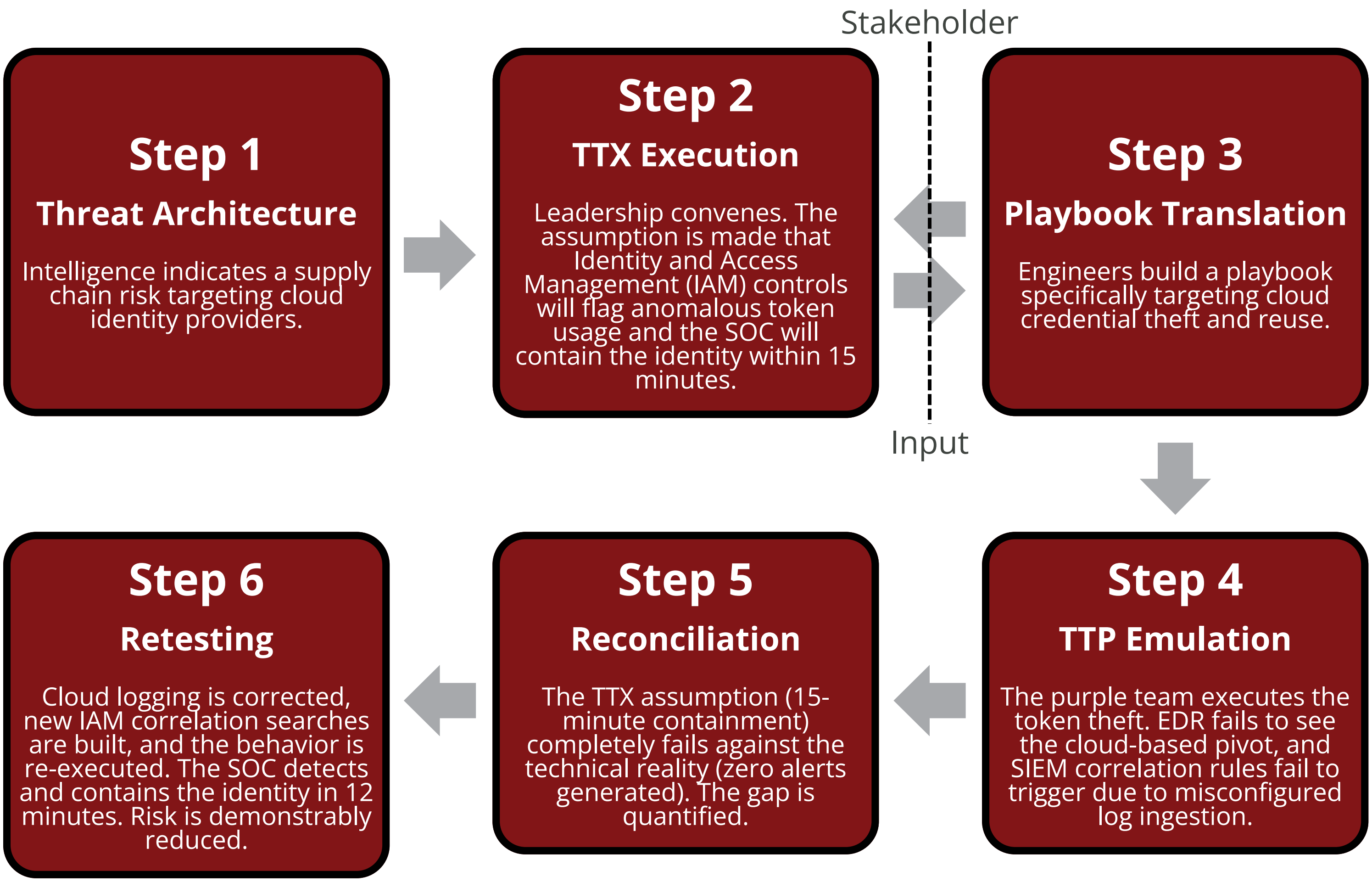
Quantitative Metrics and Measurement Framework

To properly assess the risk delta, organizations must establish Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs).

Metric Category	Target Measurement	Description
Assumption Accuracy Rate	TTX Decisions vs. Technical Reality	Percentage of technical assumptions made during the TTX that were proven true during the TTP Replay.
Response Velocity	MTTD and MTTR	Time taken for the layered security stack to detect the emulated behavior and the subsequent human response time.
Detection Fidelity	Signal-to-Noise Ratio	Evaluation of whether detection rules successfully found the signal or drowned in operational noise.
Remediation Validation	Post-Retest Success Rate	Percentage of identified visibility gaps successfully closed and validated during the Step 6 retest phase.

Case Study Simulation

Scenario: Compromise of a Critical SaaS Provider leading to Cloud Privilege Escalation.



Stakeholder

Input

Step 1

Threat Architecture

Intelligence indicates a supply chain risk targeting cloud identity providers.

Step 2

TTX Execution

Leadership convenes. The assumption is made that Identity and Access Management (IAM) controls will flag anomalous token usage and the SOC will contain the identity within 15 minutes.

Step 3

Playbook Translation

Engineers build a playbook specifically targeting cloud credential theft and reuse.

Step 4

TTP Emulation

The purple team executes the token theft. EDR fails to see the cloud-based pivot, and SIEM correlation rules fail to trigger due to misconfigured log ingestion.

Step 5

Reconciliation

The TTX assumption (15-minute containment) completely fails against the technical reality (zero alerts generated). The gap is quantified.

Step 6

Retesting

Cloud logging is corrected, new IAM correlation searches are built, and the behavior is re-executed. The SOC detects and contains the identity in 12 minutes. Risk is demonstrably reduced.

Risks, Limitations, and Organizational Barriers

Implementing this framework is not without friction

Cultural Resistance *Technical teams and business units often exist across an age-old chasm between threat and risk. Overcoming this requires transparent stakeholder feedback loops.*

Vendor Pushback *Vendors may resist objective testing of their platforms. Organizations must use TTP replays to enforce vendor accountability.*

Resource Constraints *Running comprehensive exercises requires significant capacity and time. To mitigate this, teams should prioritize the most urgent detections rather than pursuing complete framework coverage*

Simulation Believability *If a scenario lacks realism, stakeholders will reject the premise. Thorough threat-informed architecture is required to ensure alignment with actual business concerns.*

Implementation Roadmap

Days 1-30

Foundation

Identify executive sponsors, establish a governance model, and select an initial, highly probable threat scenario driven by ISAC and CTI data.

Days 31-60

Execution

Conduct a targeted TTX with cross-functional leaders, including legal and communications. Immediately document technical assumptions and translate them into a targeted TTP playbook.

Days 61-90

Validation

Perform the live-fire purple team engagement. Map the resulting telemetry back to the TTX assumptions, report the quantified gaps to the board, and initiate the remediation and retesting cycle.

Organizations can no longer afford to operate on theoretical confidence. Readiness does not emerge from polished scenarios executed in separate silos. This methodology establishes a rigorous, defensible, and regulator-aligned architecture. By bridging the strategic decision-making of a Tabletop Exercise with the empirical validation of TTP Replay, security teams transition from guessing to proving. This continuous feedback loop sharpens decision playbooks, cleans telemetry, and provides the exact evidence leadership needs to defend their security posture to boards, auditors, and regulators.

LARES

A DAMOVO COMPANY