

TotalTest Simulations v2.Oh!

From Exploits to Economics

DEF CON 33 | Las Vegas | August 10, 2025

FTI CONSULTING | CYBERSECURITY

$>WHOAMI? – Speaker Intro



Nebu Varghese

Senior Director, EMEA Cybersecurity
London, United Kingdom

Over 13 years of multi-functional experience, deep technical expertise, and strong academic credentials in the field of cybersecurity. I have worked in over 29 countries, serving a wide range of global organisations spanning across multiple sectors, including critical national infrastructure, consumer products, FS, manufacturing, renewable energy and TMT.

Qualifications:

- Certified Red Teaming Expert (CRTE)
- Offensive Security Professional (OSCP)
- CREST Registered Tester
- Computer Hacking Forensics Investigator (CHFI)
- Microsoft Azure Security Engineer (AZ-500)
- Certificate of Cloud Security Knowledge (CCSK)

- FIRST Red Teaming SIG Member
- UK National Cyber Security Center (NCSC) – Security Testing Expert Group (STEG) Member
- MSc in Software and Systems Security – University of Oxford



The Shocking Reality

Production Halted. SCADA Alarms Blaring. The CEO Demands ANSWERS..#> …….?





The Complex World WE Live In

Threats and Risks Landscape – Constantly Evolving

Keeping up with the latest threats requires ongoing investment in security awareness, training, and technology, which can be challenging for many organisations.



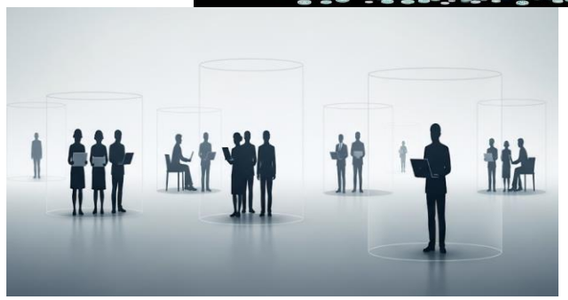
Expertise and Capabilities Required

- Organisations face challenges not only with **technically deficient** and **outdated systems**, but also **inadequate business processes**, increasing vulnerability to attacks
- The **human element**, such as susceptibility to phishing, and **unclear incident response plans**, also exacerbate security risks



Siloed Comms. and Lack of Collaboration

- Information silos between different departments hinder effective communication and collaboration during a crisis,
- Lack of practice and awareness leading to delayed response and increased damage as a result



To The Adversary's Advantage - From Heterogeneous to Homogeneous…



Current State - The Rise of Scalable Threats

The Past: Enterprise environments were once heterogeneous, with bespoke systems and unique configurations at each location. This made attacks complex and costly for adversaries, requiring tailored approaches.

The Present: The industry shifted towards homogeneity for efficiency and cost benefits. Common technologies, vendors, and architectures now dominate. This inadvertently created an environment where ransomware can scale across diverse environments.

The Consequence: ?

Theoretical Cyber and Practical Resilience – Bridging the Confidence Gap

'Can we withstand an attack?' Are we truly testing what matters to answer that question decisively?

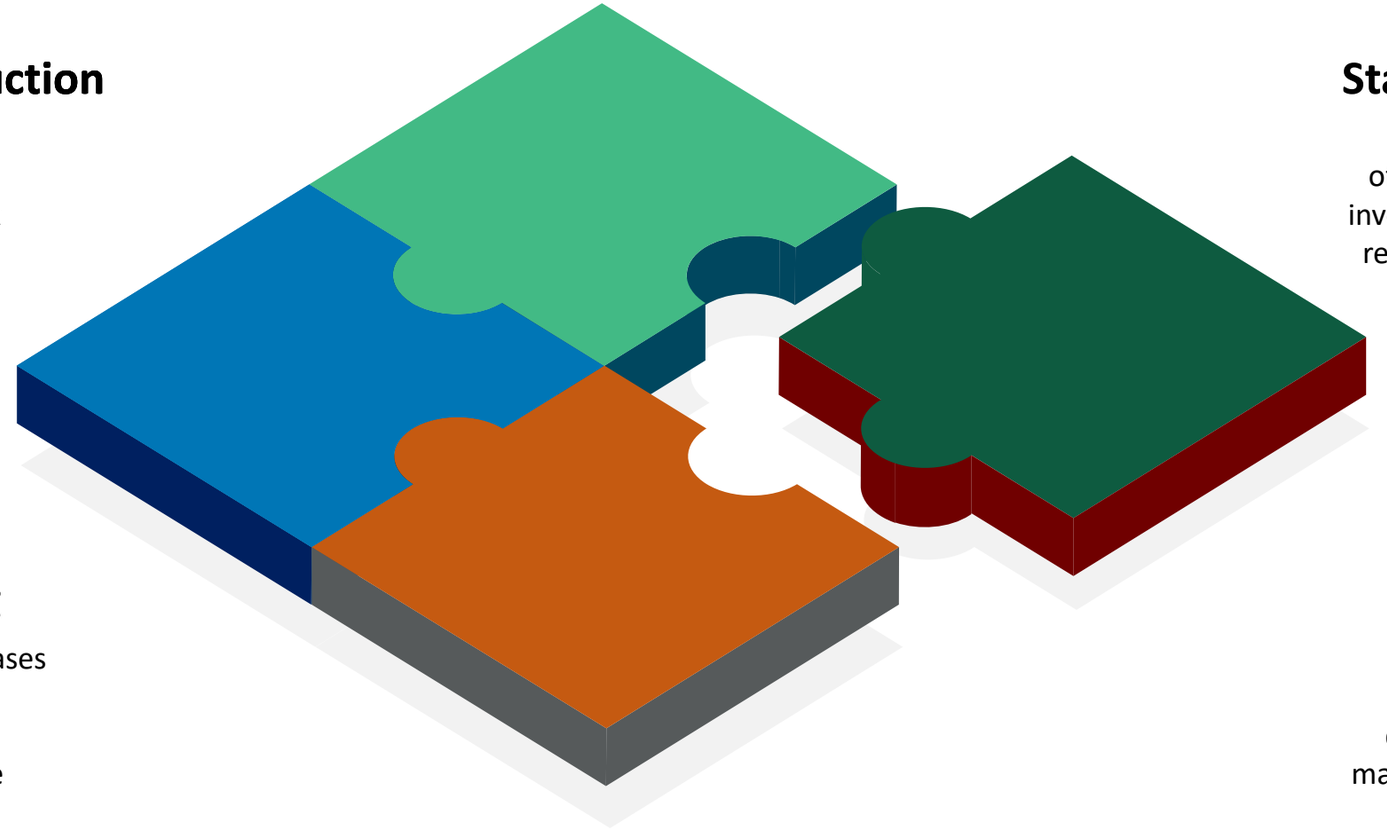
We might feel confident because our controls look robust on paper, but will they seamlessly all work together in a crisis?



TotalTest Simulations – Missing Piece?

Attack Surface Reduction

The Red team supports businesses identify / address vulnerabilities, close-off attack paths and entry points



Stakeholder Response

Tactical and Leadership teams often lack the opportunity to be involved in real-time exercising of response processes and building muscle memory.

Security Monitoring

Monitoring rulesets and use cases are significantly enhanced to improve tactical response measures and threat resilience

Defense in Depth

Address weaknesses from a network design and configurations' standpoint – to make it harder for the attacker to stage a complex intrusion

Breaking Smarter: Collaboration Brings Greater Success

Red Team

Works with CTI to develop attack plans that add the most value for every cycle.

Cyber Threat Intelligence

Work with Risk Management to prioritise scenarios. Also, identify the latest attack vectors and build relevant actor profiles

Vulnerability Management

Works with CTI to prioritise which vulnerabilities to patch first. Also, works with SOC to build safety nets around high-risk zones

Risk & Compliance

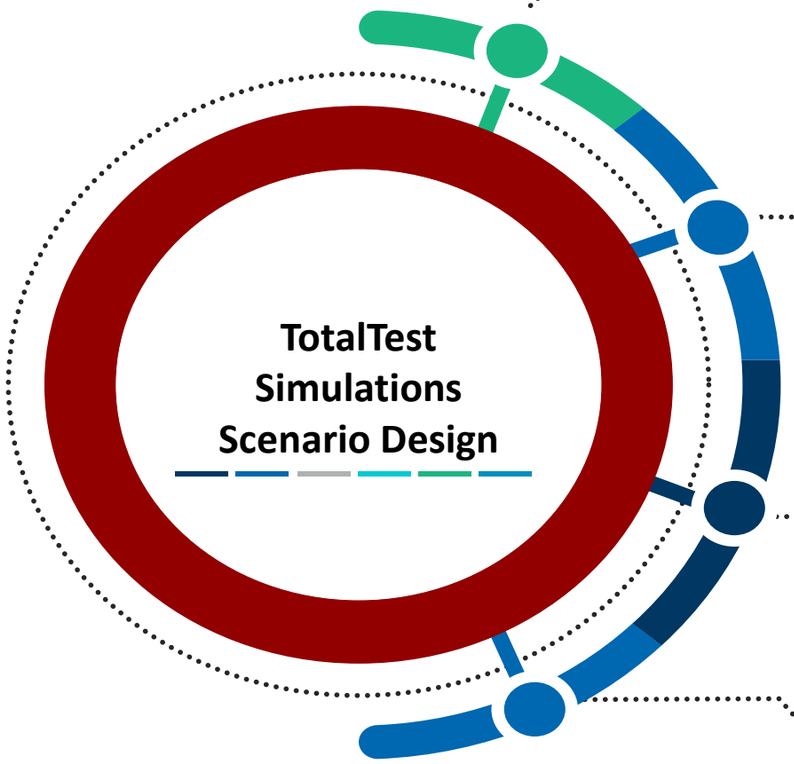
Works with key stakeholders to integrate this program into the overall risk management strategy.



Security Operations

Feedback to CTI to test less mature detection in subsequent cycles. Investigate and build response.

Architecting the Unknown: Building Scenarios for Radical Uncertainty



Dynamic Simulation Playbooks — 1

- ✓ Our offensive scenarios are built as **probabilistic state machines**, informed by real-time defensive telemetry.
- ✓ This enables our Red Team to **adapt on the fly very quickly**, mimicking sophisticated APT **decision cycles** and pushing the SOC to defend against **truly unpredictable shifts** in attack methodology, not just static scripts.

Interdependency Blind Spots — 2

Apply **fuzzing principles** at the enterprise level. Think of it as chaos engineering meets red teaming. Injecting controlled, **unpredictable inputs** or conditions into system interactions – especially across **IT/OT boundaries** – to force unexpected state transitions that exploit design flaws, not just CVEs.

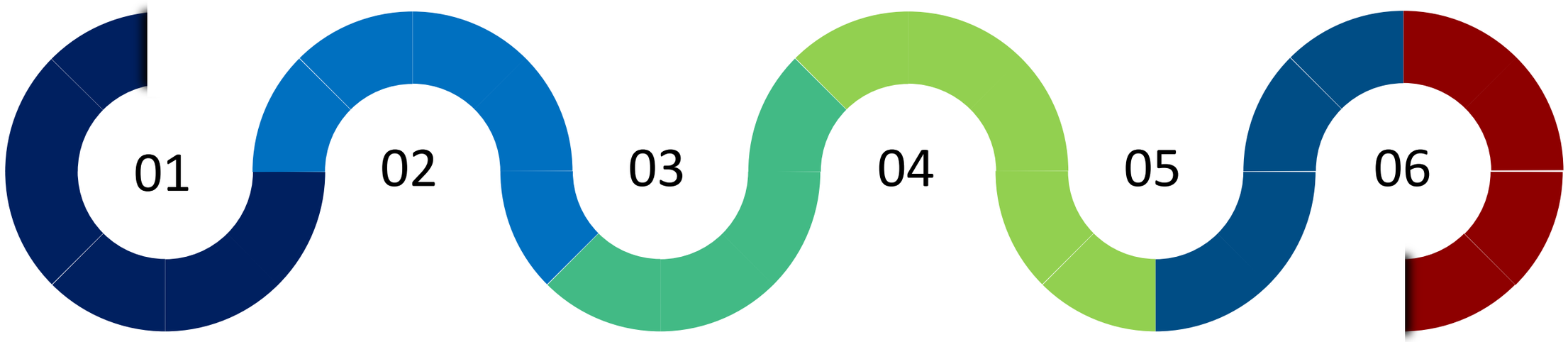
Attack Paths - Graph Theory — 3

Leveraging **graph databases** and advanced pathfinding algorithms to map complex dependencies – from identity to critical assets,. This allows to programmatically generate **novel, multi-stage attack** paths that aren't clear

Exploiting Trust Chains & Interdependencies — 4

Exploiting **subtle misconfigurations** or vulnerabilities in **federated identity** protocols. Meticulously map and attack third-party dependencies, federated identity systems, and critical **supply chain** vulnerabilities as **novel entry** points.

A Continuous Cycle of Adversary Emulation and Improvement



Define

Determine critical business units, top priority threats, major business risks and any subsidiaries needed to be in scope

Develop

CTI, VM and Internal Audit teams together and determine the most valuable scenarios

Simulate

Time-boxed end-end scenario-based simulation of attack scenario defined for the respective cycle

Workshop

Replay with SOC to identify where response could have been more quickly executed

Feedback

Relay results back to VM, CTI, IR and define improvement roadmap and milestones

Repeat

Deliver reports, project teams engaged for next steps and cycle repeat

11

Metrics Definition - Measuring Success & Demonstrating Value

A data-driven approach to quantify program effectiveness better, demonstrating tangible risk reduction and ROI over time.

TECHNIQUE COVERAGE
Percentage of ATT&CK techniques that your security tools and processes can detect and prevent

TIME TO EXPLOIT
Average time the red team takes to obtain an initial foothold

LATERAL MOVEMENT SUCCESS RATE
(Success Vs Fail) % during red team events within AD and IT/OT environments

TIME TO CONTAIN
Average time it takes to isolate and contain an attack once it has been detected.

VULNERABILITY DISCOVERY RATE
Average # of critical severity observations discovered per matter

EXPLOITATION SUCCESS RATE
Average # of critical vulnerabilities identified and exploited per test

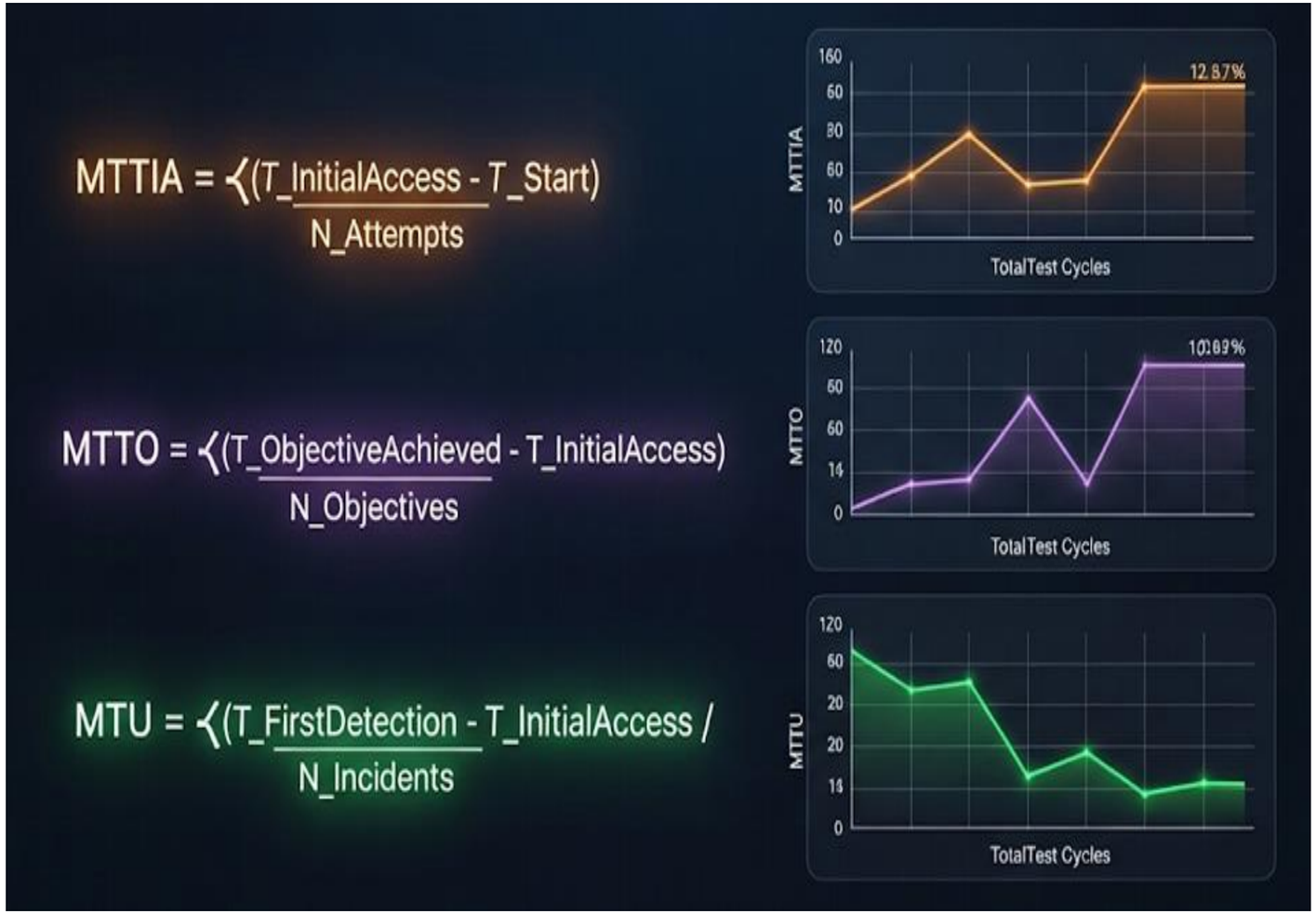
TIME TO DETECT
Average time it takes for the SOC or built-in tooling to detect specific ATT&CK techniques

TIME TO ESCALATE
Median time to successfully escalate privileges after obtaining an initial foothold

ATTACK SURFACE REDUCTION (ASR %)
On an average, % reduction in internal attack surface area – via identifying and closing off attack paths

Measuring Better: Quantifying Offensive (Red Team) Performance

Quantifying Our Offensive Effectiveness



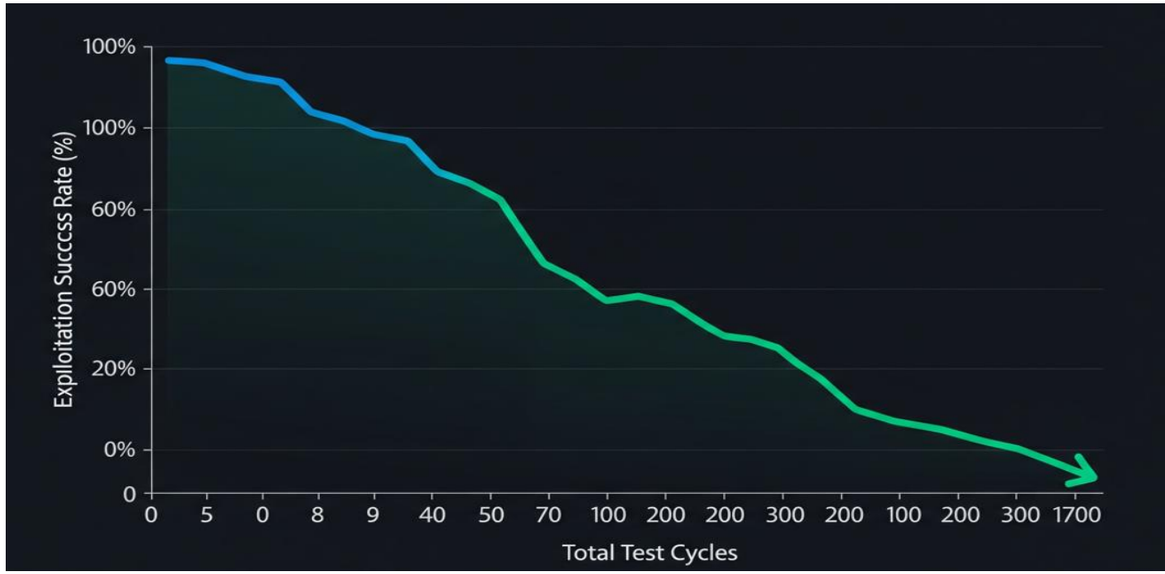
Mean Time to Initial Access (MTTIA): How long did it take *the Red Team* to get in? *(We want this to increase over cycles - means defenses are getting better).*

Mean Time to Objective (MTTO): How long did it take *the Red Team* from initial access to objective? *(An increase - means internal defenses are getting better).*

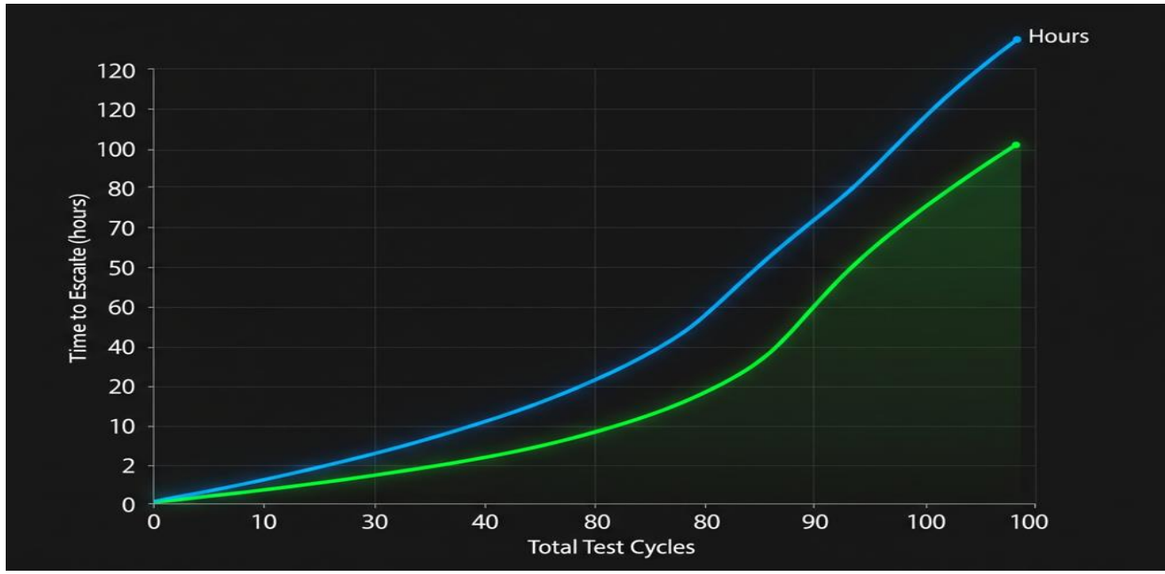
Mean Time Undetected (MTU): How long did *we* operate before detection? *(We want this to decrease - means the SOC / Blue Team is responding quicker).*

More metrics for the Red Team

Exploitation Success Rate (ESR): ***"Average # of critical vulnerabilities identified and exploited per test."***
Integration: This measures the effectiveness of the Red Team in finding *and leveraging* critical vulnerabilities. A high number initially, followed by a decrease, shows the Blue Team patching effectively or hardening systems, forcing the Red Team to work harder ("Break Smarter").



Time to Escalate (TTEsc): ***"Median time to successfully escalate privileges after obtaining an initial foothold."***
Integration: Crucial for understanding Privilege Access Management (PAM) maturity and host-based detection capabilities. An increasing time for the Red Team to escalate indicates stronger controls.

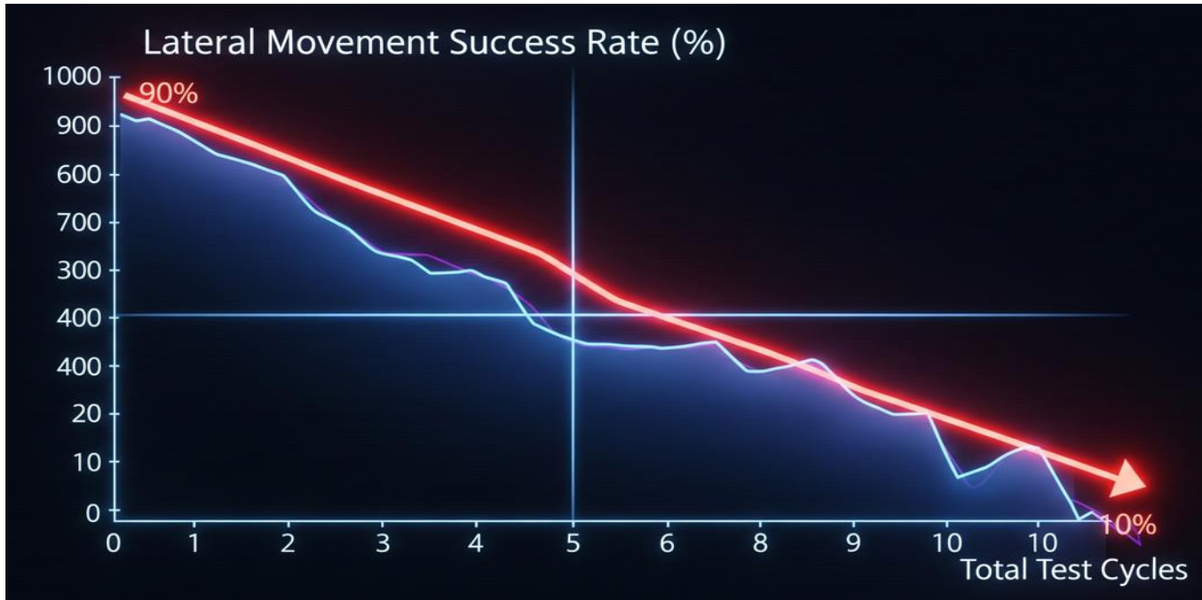


And More …….

Time to Exploit (TTE): ***"Average time the red team takes to obtain an initial foothold."***
This is very close to MTTIA but focuses specifically on the *exploit* phase. It's a fantastic metric for the Red Team to track their efficiency in bypassing initial defenses. An increasing trend means it's taking the Red Team longer to get an initial foothold, indicating stronger perimeter defenses.

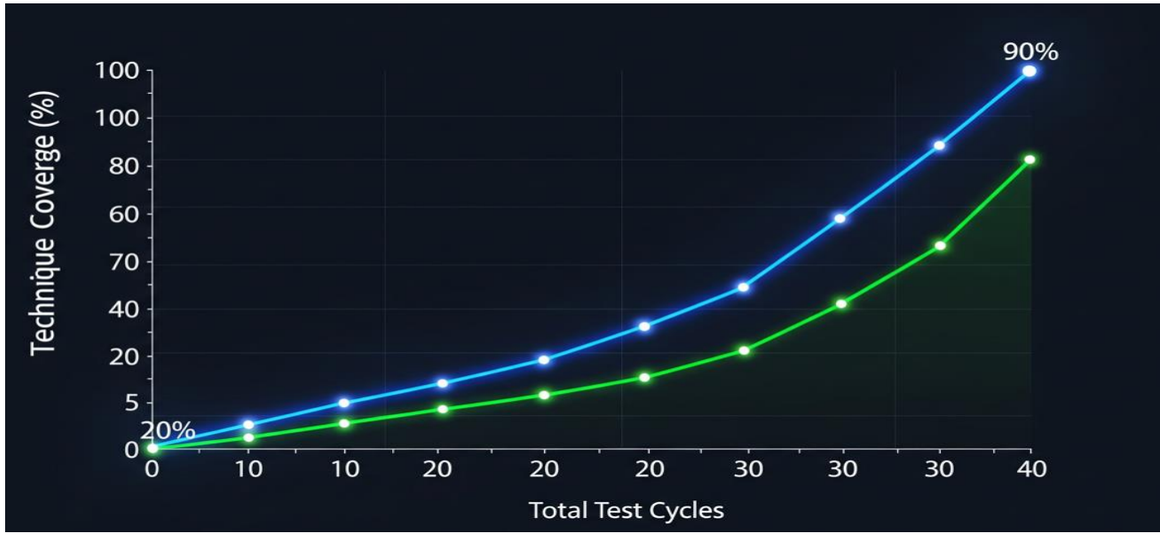


Lateral Movement Success Rate (LMSR): ***"(Success Vs Fail) % during red team events within AD and IT/OT environments."***
This directly measures the effectiveness of internal segmentation, credential hygiene, and lateral movement detection capabilities. A lower success rate for the Red Team indicates better Blue Team performance.

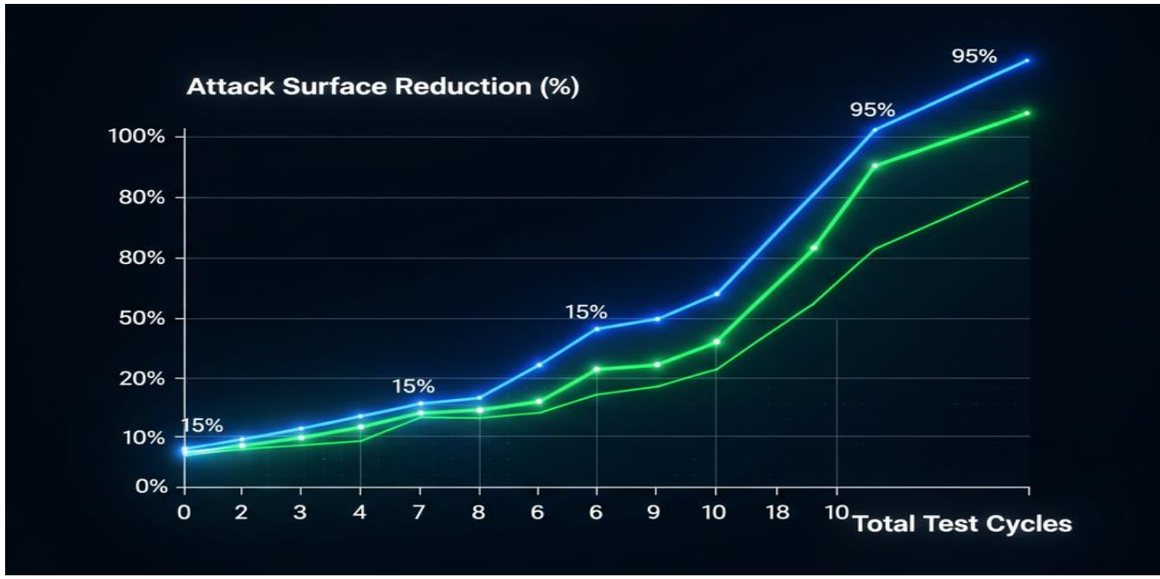


Some Indicative Metrics for the Blue Team

Technique Coverage: ***"Percentage of ATT&CK techniques that your security tools and processes can detect and prevent."***
Integration: This is a direct measure of Blue Team maturity. It directly impacts TTD and MTU. Higher coverage means faster detection, reducing 't' in the LPI.

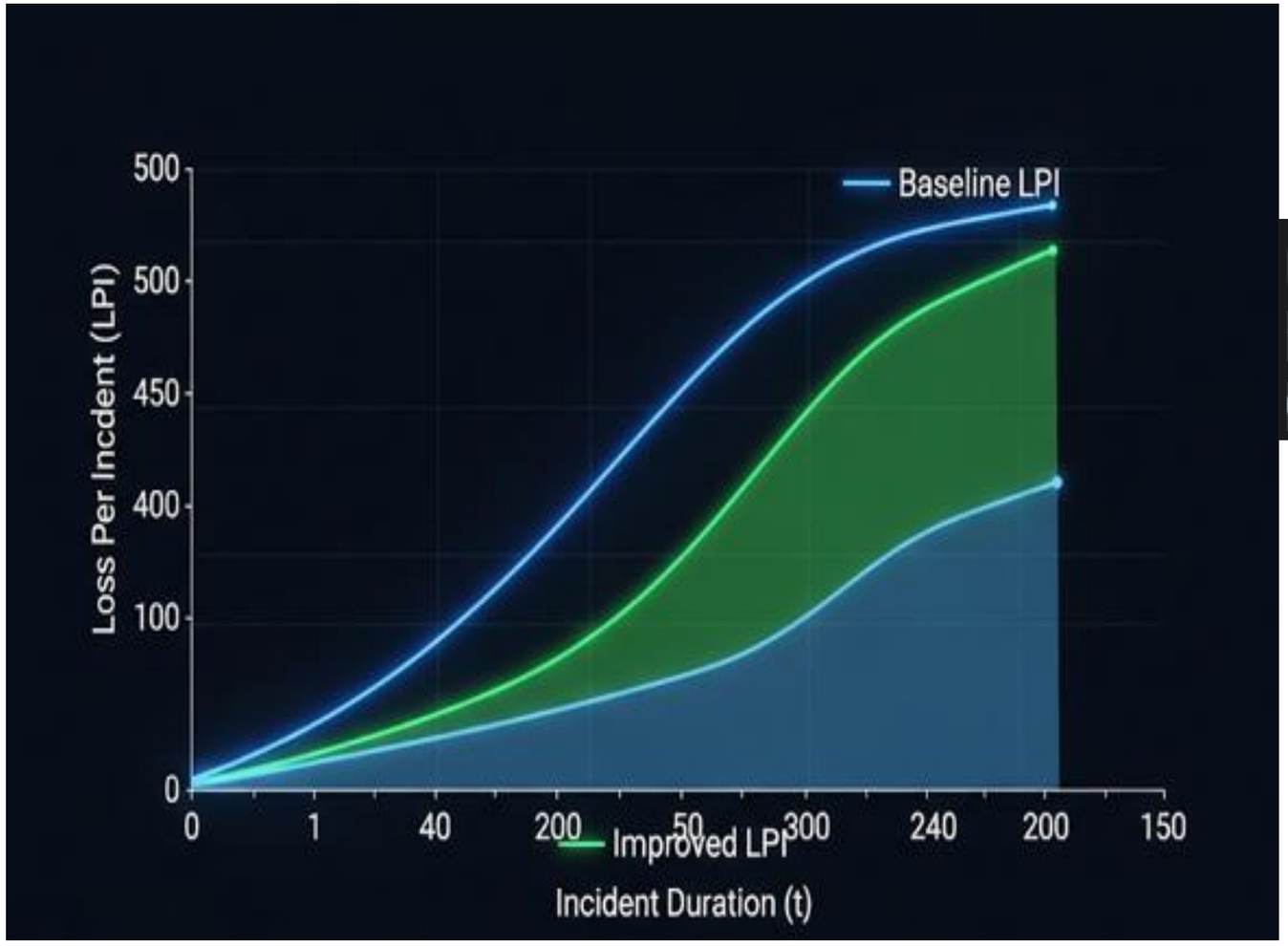


Attack Surface Reduction (ASR %): ***"On an average, % reduction in internal attack surface area – via identifying and closing off attack paths."***
•**Integration:** This is a high-level outcome metric of a robust security program, directly influenced by vulnerability remediation and network hardening driven by red team insights. It would significantly reduce MTTIA and MTTO over time.



The Economic Lens: LPI as a Time-Dependent Function

From Incident Duration to Financial Devastation: LPI(t)



"**Loss Per Incident (LPI)** isn't static. It's a critical function of t, the **total duration of the incident's impact**. Our offensive simulations and blue team's measured performance directly influence this t."

```
LPI(t) = C_Fixed + C_Downtime * t_Downtime + C_DataExfil_Rate *
t_Exfiltration + C_Response_Rate * t_Response + C_Escalation(t) +
C_Reputation_Impact(t)
```

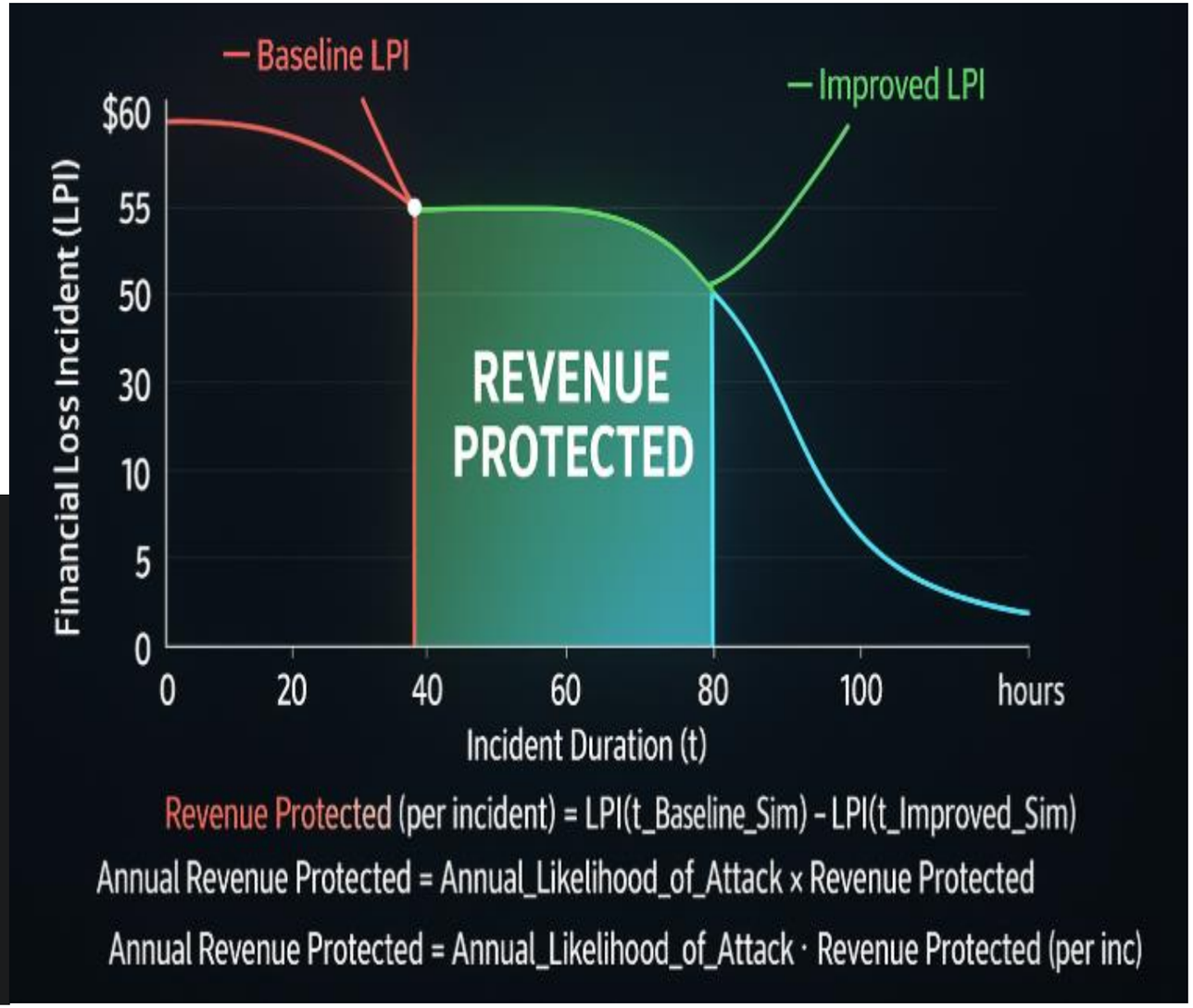
"Every minute saved off TTD, TTC, or TTE_recovery by the blue team through TotalTest cycles directly reduces the total financial bleeding from a breach."

Quantifying Revenue Protected

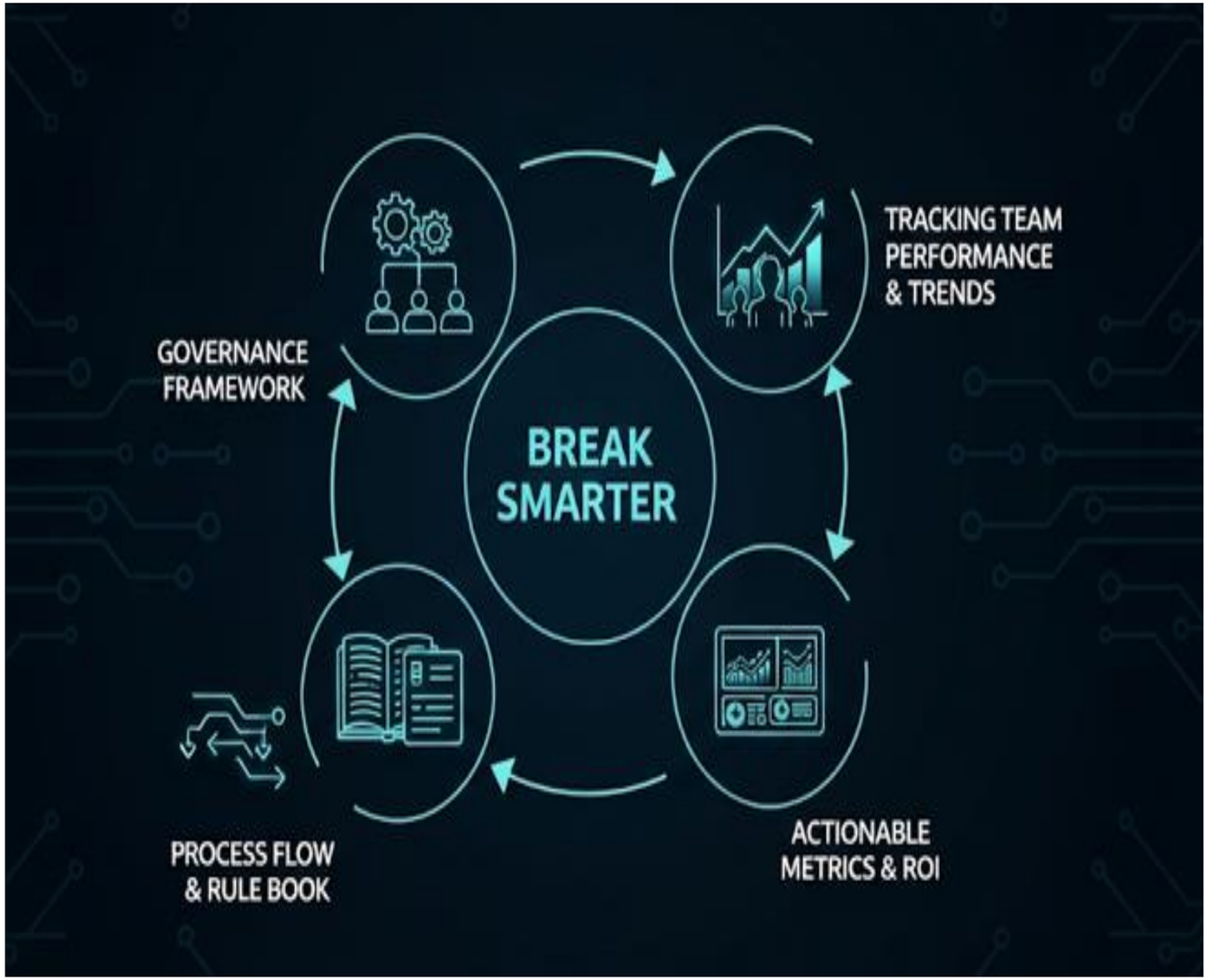
The ROI of Resilience: Calculating Revenue Protected

"This is the core economic justification. ***Revenue Protected*** *is the quantifiable financial value safeguarded by improving our defensive posture, directly measured by the reduction in potential LPI due to improved blue team performance."*

- **Revenue Protected (per incident) Formula:**
  - `Revenue Protected (per incident) = LPI(t_Baseline_Sim) - LPI(t_Improved_Sim)`
  - `LPI(t_Baseline_Sim)`: Loss from initial/worst-case simulation (before improvements).
  - `LPI(t_Improved_Sim)`: Loss from the same scenario *after* blue team improvements (measured in later TotalTest cycles).
- **Annualizing the Protection Formula:**
  - `Annual Revenue Protected = Annual_Likelihood_of_Attack * Revenue Protected (per incident)`
  - `Annual_Likelihood_of_Attack`: Informed by threat intelligence and observed MTTIA.



Practical Blueprint for Success



*"**TotalTest** is about learning, not shaming. Promote a 'blameless post-mortem' culture. Celebrate the blue team's improvements and empower the red team to continuously evolve their tactics."*

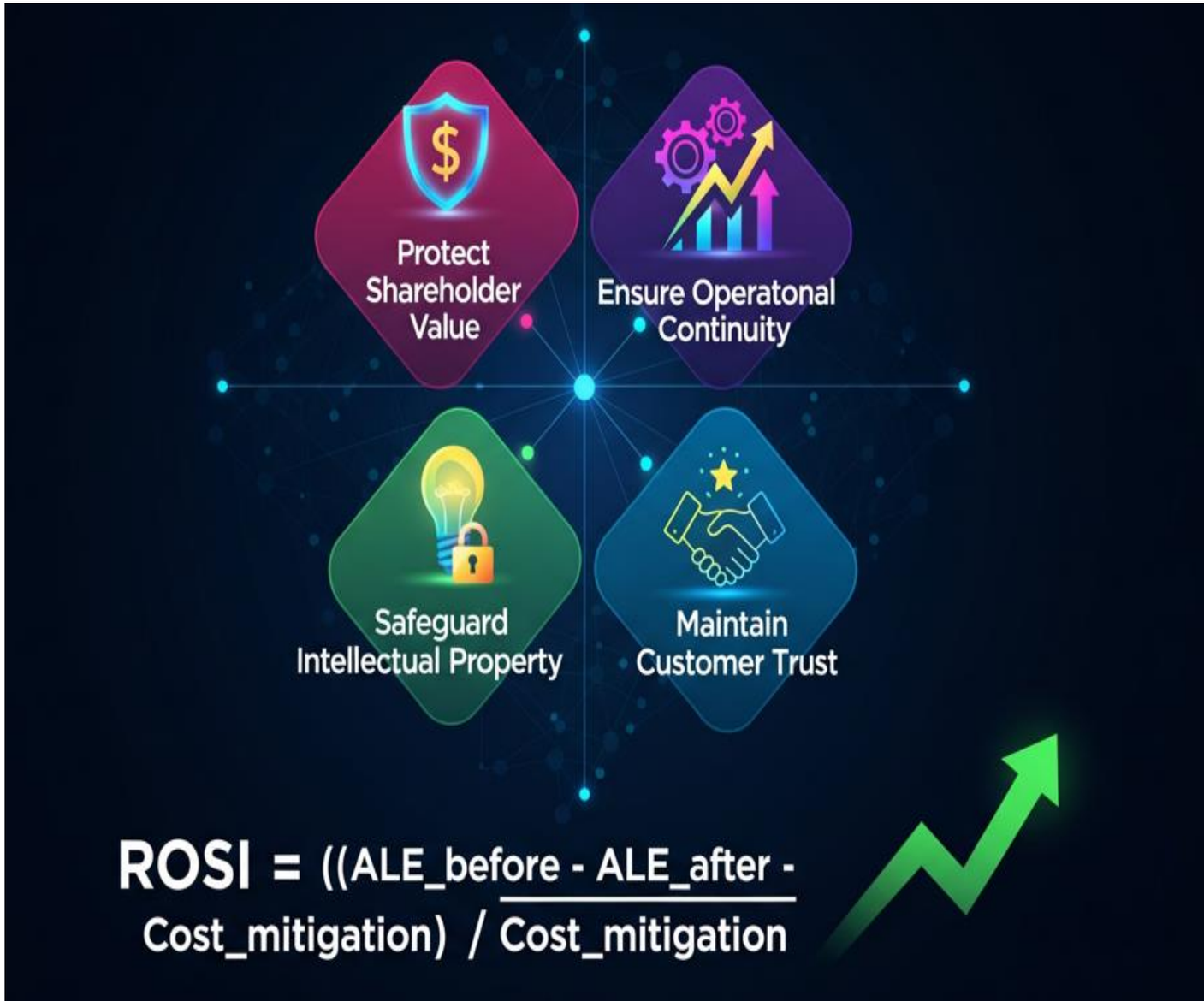
- ✓ **The Red Team** generates the technical insights. Your job, CISO, is to **translate** their 'kill chain' into 'cost avoidance' and 'revenue protection.'
- ✓ Regularly present a TotalTest **'Scorecard'** to the Board, showing trends of decreasing LPI and increasing Revenue Protected.
- ✓ Start **agile**. Focus on your **crown jewels first**. Integrate TotalTest into your enterprise risk management (**ERM**) framework.
- ✓ **Mandate cross-functional participation** from IT, OT, Legal, Comms, HR for full crisis simulation

Funding Your Fixes: Strategic Buy-In

From Cost Center to Strategic Business Enabler

"This quantifiable data is the language of the Board and CFO. TotalTest 2.Oh! provides the ***irrefutable evidence to secure sustained buy-in and funding*** *for critical security improvements."*

Risk Appetite Dialogue: Our precise, simulation-driven LPI calculations allow for a fact-based discussion about the Board's *actual* cyber risk appetite.



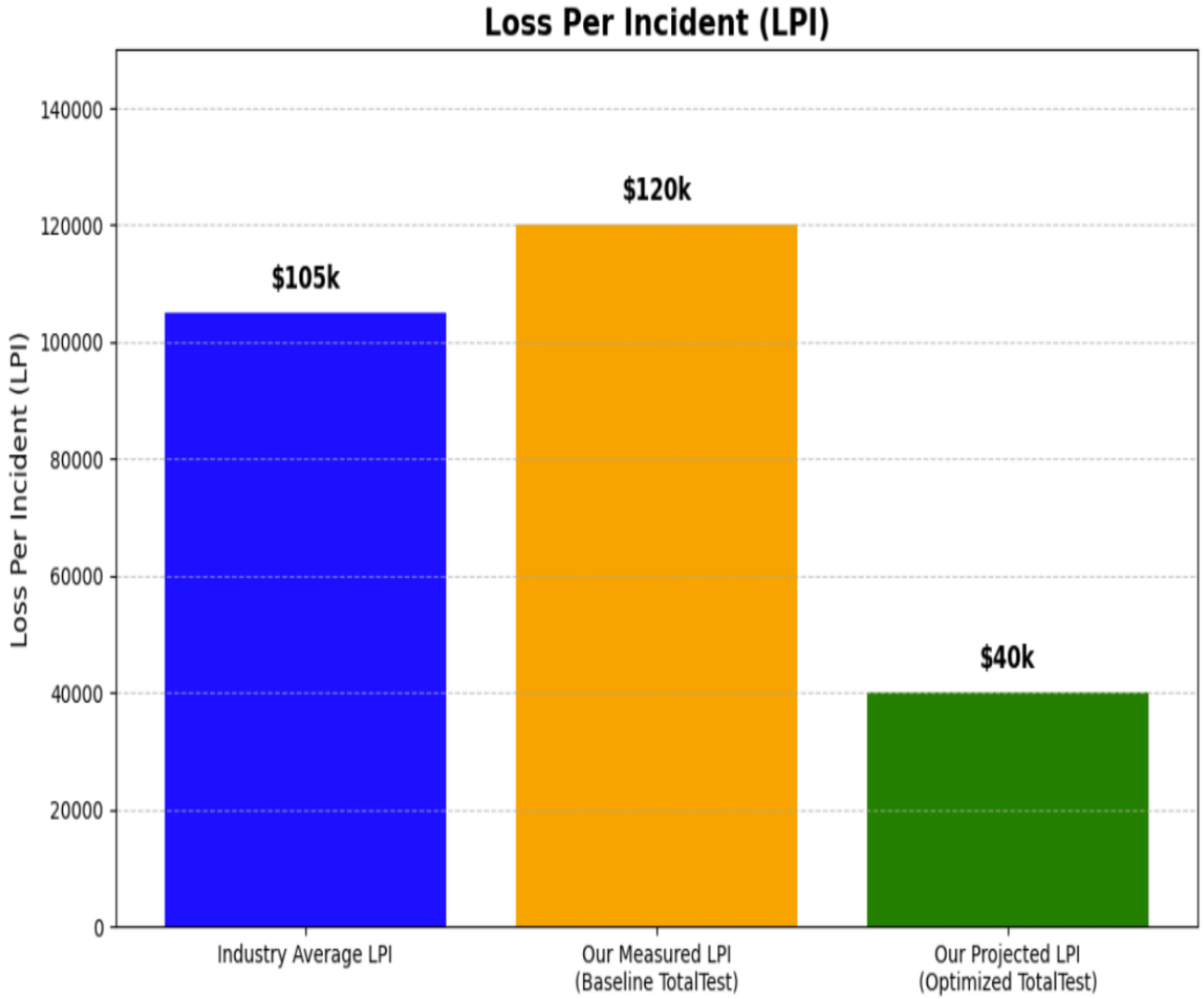
Benchmarking for Board-Level Authority

Beyond Averages: Proving Superior Risk Posture

*"**Benchmarking** against industry data provides crucial external validation for the Board and CFO, identifying opportunities to 'stand out' where it counts."*

Data Sources: *IBM's Cost of a Data Breach, Verizon DBIR, sector-specific ISAC/Ponemon reports.*

- **Working Backwards & Normalization Formula:**
  - `Adjusted LPI (Your Org) = Industry_Average_LPI * (t_Actual / t_IndustryAvg)`
  - "If our `t_Actual` is significantly lower, our residual financial risk from breaches is demonstrably lower than our peers – a competitive advantage."
- **Cyber Insurance Implications:** Quantified, demonstrated risk reduction can also lead to lower cyber insurance premiums.





Questions

Thank You