The Offensive Security Buyer's Playbook:

MAXIMIZING ROI

Sprocket Security | www.sprocketsecurity.com

MESSAGE FROM THE COO

Gaurav Kulkarni
Chief Operating Officer
Sprocket Security

Gaurav Kulkarni

In today's security landscape, buying security solutions has become as challenging as defending against threats. Every vendor promises innovation, automation, and value, but few deliver measurable outcomes that truly strengthen resilience.

At Sprocket Security, we built our approach around the belief that it matters what your vendor proves, not just claims. We've seen firsthand that the organizations achieving the greatest security return on investment (ROI) share one defining trait: they lead with purpose. They treat procurement not as a transaction, but as a strategy. They ask better questions, demand transparency, and expect proven results, not promises.

We talk to hundreds of CISOs and security leaders every year, and their message is clear: value must be visible. Budgets are under pressure, teams are stretched thin, and leadership needs proof that every dollar invested in security produces measurable improvements.

This playbook was created to help leaders procure offensive security solutions with precision, measure ROI with confidence, and turn testing into a competitive advantage. Whether you're buying your first engagement or optimizing a mature program, the goal is the same: navigating the offensive security marketplace with clarity, confidence, and making every decision data driven.

Strong security isn't about buying more tools. It's about proving what works.

TABLE OF CONTENTS

CHAPTER #1

INTRODUCTION

Security buyers are fatigued by vendor promises that all sound the same; “reduce risk”, “automate faster”, or “deliver the best ROI”. Meanwhile, security teams struggle with shrinking budgets and the constant question from leadership, “What’s actually working?”

That’s why offensive security solutions stand out. They reveal in real time how resilient your defenses really are by exposing them to real adversarial conditions. The results provide a means to justify your investments and give you hard evidence to demonstrate what is effective. Even though offensive solutions deliver real results, most organizations struggle to buy, implement, and measure them effectively. Too many engagements produce surface-level reports instead of actionable insight. Too many vendors promise an all-in-one solution that magically fixes everything but can’t back it up with human expertise or measurable outcomes.

You don’t need a CISO title to lead procurement with confidence. Leadership in this process comes from knowing what your organization needs, asking better questions, and demanding proof of value. This playbook draws from real lessons learned by security leaders who’ve done exactly that: evaluating partners, tracking ROI, and turning offensive security into continuous improvement.

By the end, you’ll have a clear framework for:

- *Cutting through vendor noise to focus on measurable results.*
- *Aligning internal stakeholders around offensive security’s business value.*
- *Communicating ROI in a way that earns executive trust and sustained investment.*

Because real security isn’t about buying more tools. It’s proving what works, improving what doesn’t, and leading with evidence.

CHAPTER #2

LEADERSHIP MINDSET IN SECURITY PROCUREMENT

It's easy for security procurement to fall into the rhythm of identifying a tool, deploying it, and checking the box. The leaders who drive real impact, though, are shifting toward a model focused on measurable results. They use offensive testing data not just to find vulnerabilities, but to prove that security investments are delivering measurable improvement. The mindset must shift to "investing in resilience, measurable outcomes, and sustained improvement".

True leadership in procurement starts with clarity. Before you evaluate vendors, you define success: What do you want to prove? How will you measure improvement? Success might look like fewer exploitable paths, faster remediation, or validated improvements in detection and response. The goal isn't just to acquire new solutions. It's to build measurable confidence in your organization's ability to withstand real-world attacks.

"If you can't measure it, you can't defend it. That includes your security spend."

Phil Wong, Managing Director, Cybersecurity at Redapt

This approach is critical in today's environment. Security leaders face rising expectations with limited budgets, and the average cost of a breach reached nearly $4.9 million in 2024. When organizations adopt metrics-based security programs, like tracking ROI, risk reduction, and business alignment, they are significantly more likely to secure or grow budget. That means every decision and every dollar must deliver visible, defensible value.

Strong leaders engage directly in procurement, asking tough questions, and ensuring every investment supports measurable outcomes. They balance innovation with stability, exploring new offensive techniques and tools while maintaining control, visibility, and repeatable processes.

“Offensive security isn’t about checking a compliance box. It’s about validating how resilient you really are when it counts.”

Casey Cammilleri, CEO of Sprocket Security and host of Ahead of the Breach podcast (episode 1)

Leadership’s mindset in procurement means moving from “What can we buy?” to “What can we prove?” It’s about aligning stakeholders around the shared goal of measurable resilience. Every purchase becomes a data point in how the organization learns, adapts, and strengthens its security posture. Offensive security delivers ROI not by finding weaknesses, but by proving progress.

CHAPTER #3

HOW TO EVALUATE OFFENSIVE SECURITY SOLUTIONS

The offensive security market is full of options, each promising faster results, deeper insight, and smarter automation. But leaders who achieve real ROI know that evaluation isn't about who has the best demo; it's about who can prove measurable impact on your organization's risk posture.

The first step in understanding what types of solutions exist and how they complement one another. Offensive security isn't one service. It's an ecosystem of validation methods that, when combined, give you a clear picture of how resilient your defenses really are.

TYPES OF SECURITY SOLUTIONS

PENETRATION TESTING

The foundation of most offensive programs.

- ***CPT (Continuous Penetration Testing):*** *Always-on testing that adapts as your environment changes, ensuring ongoing visibility and faster remediation.*
- ***Point-in-Time:*** *Traditional annual or compliance-driven tests to uncover exploitable vulnerabilities.*

	CPT	Point-in-Time
Human Testers	✓	✓
Compliance	✓	✓
Always On	✓	✗
Always Active	✓	✗
Change-Driven	✓	✗
Testing Breadth	✓	✗
Testing Depth	✓	✓

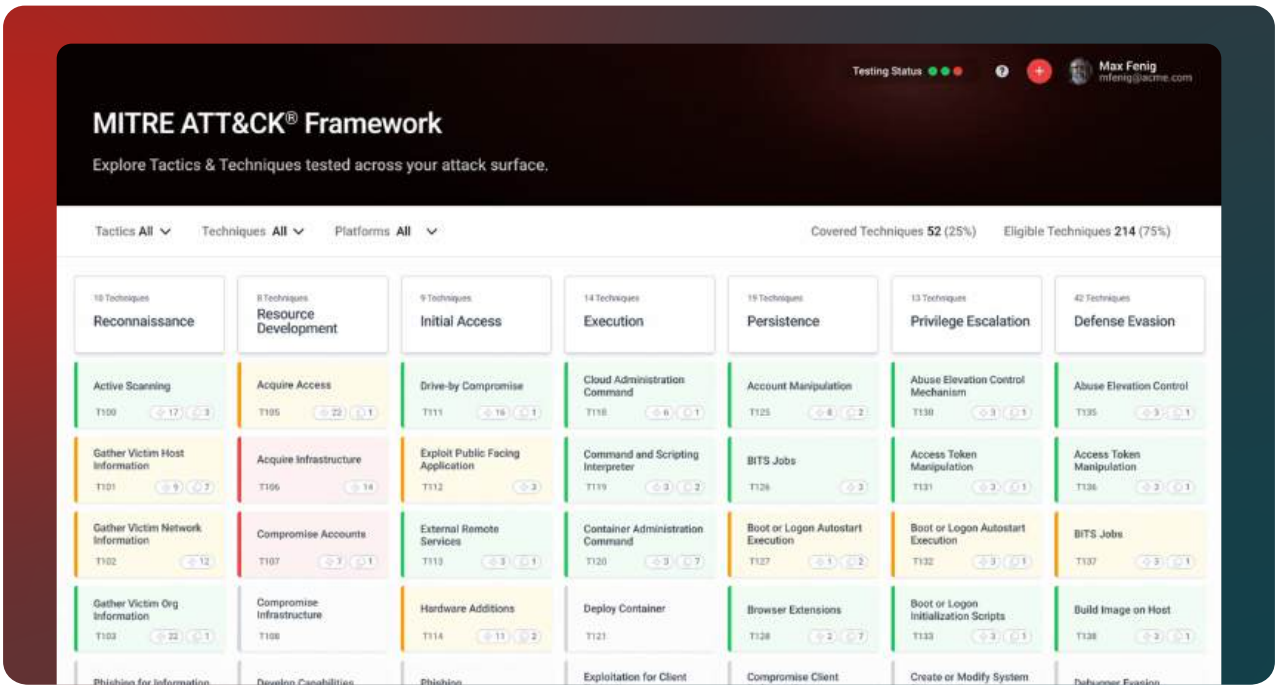
RED TEAMING

Red teaming simulates real-world attacks across people, processes, and technology. Unlike a pentest, which identifies vulnerabilities, red teaming focuses on objectives, such as gaining access to sensitive data or compromising high-value assets. The output isn't just a list of flaws, but a roadmap of how an adversary could exploit them.

ADVERSARY SIMULATIONS

These engagements test specific tactics, techniques, and procedures (TTPs) aligned to frameworks like MITRE ATT&CK. They bridge the gap between a red team's realism and a pentest's precision, helping validate your SOC's detection and response capabilities.

When mapped to frameworks like MITRE ATT&CK, adversary simulations offer repeatable, measurable testing that directly supports ROI reporting. Leaders can show progress across known adversary behaviors. The image below from the Sprocket Platform heat-map view illustrates exactly how ethical hackers can test against specific MITRE ATT&CK techniques in the live environment.



ATTACK SURFACE MANAGEMENT (ASM)

ASM continuously identifies, maps, and monitors external assets and exposures, essentially showing you what attackers see. It's the intelligence layer that drives smarter testing. But effective ASM goes beyond asset discovery. It gives security teams context on what's most exploitable and to remediate where it matters most.

TYPICAL ASSETS INCLUDE:

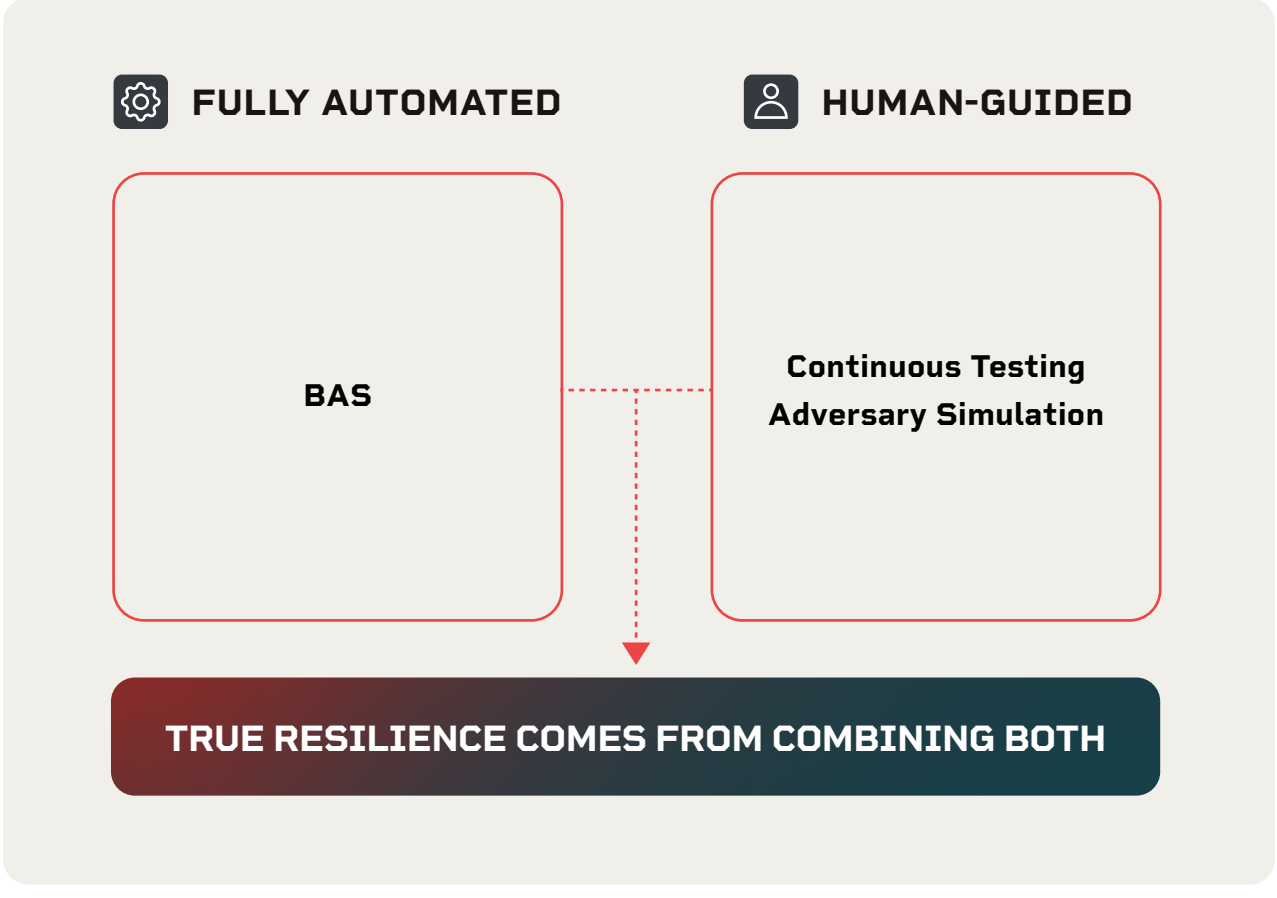
- *Domains and subdomains*
- *Web applications and APIs*
- *Cloud instances and storage buckets*
- *IP ranges and exposed services*
- *Certificates and DNS records*
- *Third-party or shadow assets*

Even as 90% of U.S. enterprise organizations say they've seen an increase in impactful attack-surface incidents, most still report weak ASM programs.

BREACH & ATTACK SIMULATION (BAS)

BAS platforms automate recurring control validation, testing how your defenses respond to common attack scenarios across network, email, and endpoint vectors.

These tools are valuable for scale, but leaders must remember automation doesn't replace human adversarial creativity. BAS helps measure resilience, but the real ROI comes when automation supports, not replaces, expert-led testing.



KEY EVALUATION FACTORS

When evaluating vendors, the best leaders think beyond the feature lists. They look for proof of value and alignment with business outcomes.

- ***Problem fit*** *– Does the solution validate your real risks, or just create more noise with generic vulnerability lists?*
- ***Depth vs Frequency*** *- Does it offer only point-in-time insight, or continuous validation as your environment evolves?*
- ***Differentiation*** *– What makes this vendor's approach or methodology distinct in a crowded market?*
- ***Integration with Security Program*** *– Will findings integrate with your existing security stack (SIEM, SOAR, ticketing, vulnerability management)?*
- ***Proof of Value*** *– Can the vendor demonstrate impact through case studies, measurable ROI metrics, or successful pilots?*
- ***Reporting and Metrics*** *– Does their output map directly to your KPIs, frameworks, and board-level reporting needs?*

When it comes to vendor evaluation, one guiding principle stands out: **Leaders should evaluate vendors not just by what they find, but by how their insights accelerate measurable improvement across the security lifecycle.**

RED FLAGS TO WATCH FOR

- *Over-reliance on automation or "magic dashboards" that lack human validation*
- *Unclear pricing or overly complicated service tiers*
- *Limited transparency in methodology or tooling*
- *No roadmap alignment with your program's maturity*

LEADERSHIP IN THE BUYING JOURNEY

Problem Identification: *Where are we blind today? (e g, attack surface visibility, control validation)*

Internal Advocacy: *Gain alignment with security, IT, risk, and compliance teams*

Validation: *Run a POC or pilot engagement to prove impact on risk reduction ademedlation speed*

Approval Process: *Tie outcomes to compliance, ROl, and resilience metrics*

Consensus Building: *Show executives how offensive security validates existing investments and reduces wasted spend*

For structured due diligence, leverage frameworks like the NIST Cybersecurity Supply Chain Risk Management (C-SCRM) Quick-Start Guide, which outlines how to evaluate and monitor security partners for integrity, reliability, and performance.

Evaluating offensive security vendors is as much about leadership as it is about testing. The goal isn't to buy another tool. It's to invest in measurable improvement. When you lead with that mindset, you move beyond comparison charts and marketing claims to what really matters: proof that your defenses can stand up to the test.

CHAPTER #4

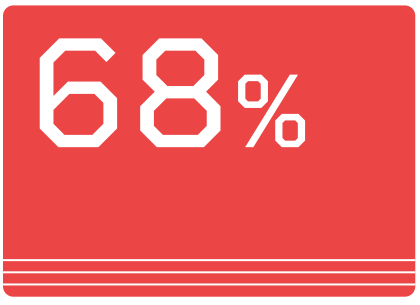
RENEWAL, REPLACEMENT, AND RISK

Every leader eventually asks the same question: **Does this vendor still deliver value worth the spend?**

In offensive security, that question carries even more weight. Continuous validation, measurable improvement, and transparent results are what separate a strategic partnership from a transactional service. Renewal should be earned.

EVALUATING ENGAGEMENT VALUE

Start by examining whether the work still drives meaningful outcomes. Are tests uncovering critical attack paths that genuinely reduce risk, or have findings become repetitive and shallow?



According to the 2024 Verizon Data Breach Investigation Report, 68% of breaches are caused by repeat vulnerabilities. Issues that had already been identified but not fully remediated. That statistic underscores why ongoing offensive testing must focus on actionable findings and follow up.

ADOPTION AND ACTION

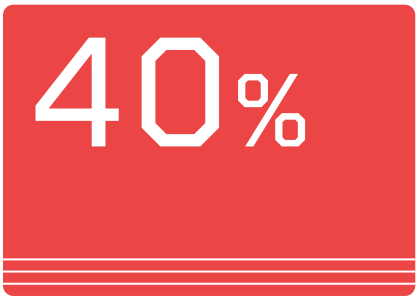
Value doesn't stop at discovery. It depends on the execution. The insights from offensive engagements should drive measurable change in how quickly and effectively vulnerabilities are closed. If reports are sitting untouched or integrations aren't feeding into remediation workflows, the ROI disappears.

Leaders should ensure testing outputs flow directly into operational systems, like vulnerability management tools, ticketing platforms, or SIEMS, so every finding becomes part of a closed-loop process.

PROVING ROI OVER TIME

Offensive security should pay for itself in measurable terms. Over time, you should be able to show:

- ***Risk Reduction (%)*** *– The decrease in exploitable findings year over year.*
- ***Time to Remediate*** *– The average time between discovery and fix.*
- ***Detection Improvement*** *– The increase in attacks detected during simulations or red team engagements.*
- ***Compliance Alignment*** *– How testing contributes to meeting or exceeding audit and regulatory expectations.*



According to ASIS International (2025), organizations that measure security performance using business metrics (such as reduced exposure or remediation speed) are 40% more likely to maintain or increase their security budgets year-over-year.

SIGNS IT'S TIME TO MOVE ON

Even the strongest vendor relationship can plateau. Knowing when to pivot is a mark of maturity, not failure. Watch for these warning signs:

- ***Poor Responsiveness or Transparency*** *– The vendor can't clearly explain findings, methodologies, or remediation timelines.*
- ***Inability to Scale*** *– The engagement model doesn't evolve as your business or attack surface grows.*
- ***Security Concerns or Audit Gaps*** *– Vendors that fail to maintain certifications, retest fixes, or validate improvements create unnecessary risk.*

Renewal and replacement decisions are where ROI becomes reality. Offensive security programs that start strong can drift without clear measurement, accountability, and communication.

As a guiding principle: Leaders should establish baseline ROI metrics in year one and require vendors to demonstrate continuous improvement against those benchmarks.

The organizations that treat renewals as opportunities for recalibration build long-term resilience, operational maturity, and measurable proof that their security investments are working.

CHAPTER #5

VENDOR RELATIONSHIPS & EXPECTATIONS

Once the contract is signed, it's time to lean in. The value of an offensive security depends as much on the relationship as on the test itself. Leaders who set clear expectations and maintain accountability turn vendors into strategic partners instead of one-time service providers.

SET THE TONE

The way your vendors engage with your organization starts with you. Leaders define what "good" looks like early. Transparency in reporting, responsiveness in communication, and alignment to your goals are all important. That means no black boxes, no vague metrics, and no surprises.

"Set-and-forget doesn't work in security. When vendor relationships are left on autopilot, performance drifts, quality slips, and ROI disappears. The long-term values comes from active engagement through regular reviews, shared metrics, and honest communication."

Mike Miller, vCISO at Appalachia Technologies

In offensive security, that level of partnership matters even more. Testing is iterative. It's not about running a single assessment and filing a report. The best vendors function like an extension of your internal team: challenging assumptions, recommending improvements, and helping prioritize what matters most.

TRANSPARENCY AND ALIGNMENT

Transparency isn't optional; it's the foundation of trust. Vendors should be open about their methodology, tooling, limitations, and data handling practices. Alignment is equally critical. Your offensive security provider should understand your environment, your regulatory landscape, and your business priorities.

ACCOUNTABILITY IS LEADERSHIP'S RESPONSIBILITY

Strong leaders don't delegate vendor accountability. They build it into the relationship from day one. That means scheduling Quarterly Business Reviews (QBRs) not as box-checking exercises, but as collaborative sessions focused on ROI, continuous improvement, and roadmap alignment.

Each QBR should address:

- ***Performance Review:*** *Are engagements meeting agreed-upon KPIs or ROI targets?*
- ***Remediation Impact:*** *How have findings influenced your organization's risk posture?*
- ***Roadmap Updates:*** *Is the vendor's evolution aligned with your security and business objectives?*
- ***Support Quality:*** *Are response times and communication levels consistent and transparent?*

FROM VENDOR TO PARTNER

The most successful offensive security programs evolve into partnerships. Partnerships means shared goals, open communication, and mutual accountability. It's about collaboration before, during, and after each engagement.

As best practice, leaders should document mutual expectations including agreed-upon success metrics or ROI indicators, communication cadences, transparency commitments, and a joint roadmap session to align on emerging threats and technology changes. When vendors are treated like true partners, they're more invested in outcomes and not just outputs. The result is strong testing, faster remediation, and a relationship built on evidence, not assumptions.

Vendor management is where leadership is tested most. The difference between a vendor and a partner comes down to transparency, accountability, and shared purpose. Leaders who treat offensive security as an ongoing collaboration gain continuous value, measurable ROI, and stronger resilience across their programs.

In other words, you don't just manage vendors. You lead them.

CHAPTER #6

MISTAKES TO AVOID

Even the strongest security programs can falter if the buying process loses discipline. Offensive security is about precision and validation. Leaders who avoid the following pitfalls not only protect their budgets but ensure that every engagement produces measurable outcomes.

NO CLEAR OWNER

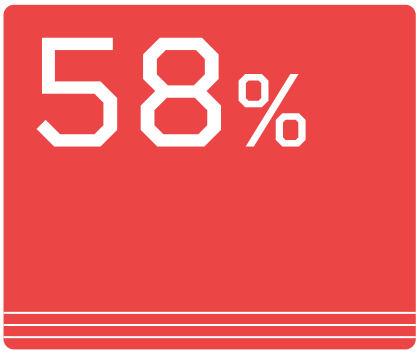
One of the most common missteps is buying a solution with no defined owner inside the organization. Without a leader accountable for strategy, execution, and follow-up, engagements drift, reports collect dust, and value erodes. Every offensive security investment should have a clear owner. Someone responsible for ensuring results drive real change, not just compliance satisfaction.

IGNORING INTEGRATION COSTS AND COMPLEXITY

Procurement decisions often focus on the proposal price, not the operational cost. If findings, reports, or data can't easily integrate into existing systems, the results won't translate into action. Integration challenges can consume more resources than the test itself, so leaders must confirm compatibility early in the evaluation process.

BUYING THE HYPE

In a crowded market, it's easy to be drawn in by buzzwords. "AI-powered," "automated," or "next-generation." But leadership means filtering signal from noise.



According to Forbes Technology Council (2024), 58% of cybersecurity leaders admit they've purchased tools that were underutilized or redundant within 18 months. The fix? Buy based on proof, not promise. Demand measurable ROI and evidence that the solution strengthens your specific risk posture, not someone else's.

SKIPPING DATA PROTECTION NEGOTIATIONS

Data protection isn't a fine-print issue. Before signing, confirm how the vendor handles sensitive data, test artifacts, and customer information. Contracts should include explicit terms for **breach notification, data retention, secure destruction, and compliance alignment** with frameworks, like GDPR or HIPPA.

If those clauses aren't clear, the risk transfers directly to your organization.

RUSHING PROCUREMENT UNDER PRESSURE

When budgets or audits loom, leaders may feel compelled to "just get something in place." But rushing procurement almost always costs more later. Quick decisions often lead to poor fit, limited scalability, or integration failures. The most effective leaders slow down at the start. Define problems clearly, validate claims through proof-of-concept testing, and document ROI expectations before approval.

ASSUMING AUTOMATION EQUALS COVERAGE

Automation is valuable, but it isn't comprehensive. Breach and Attack Simulation (BAS) platforms and vulnerability scanners can accelerate detection, but they can't replicate human intuition or creativity.

A hybrid approach works best: automation for consistency, **human adversarial testing** for depth and realism. Real attackers don't follow scripts, and neither should your testing program.

FAILING TO RETEST AFTER REMEDIATION

Finding a weakness isn't the same as fixing it. Without validation, ROI becomes theoretical. Each round of testing should include targeted retesting of previously identified issues to confirm effective remediation. Continuous validation transforms testing from a snapshot into a measurable improvement cycle.

Procurement mistakes don't just waste money, but they create false confidence. The organizations who consistently get value from offensive security programs share one trait: they treat every step as an opportunity to measure, refine, and prove progress. In other words, success isn't in the purchase. It's in the follow-through.

CHAPTER #7

10 QUESTIONS TO ASK EVERY OFFENSIVE SECURITY VENDOR

10 QUESTIONS TO ASK EVERY OFFENSIVE SECURITY VENDOR

1. *How does your solution specifically address **our top security risk and threats?***
2. *Can you provide **customer references** from an organization like ours that **demonstrates the measurable ROI** you've delivered for them?*
3. *How do you integrate with **our existing technology stack** (tools, processes, workflows) or **compliance frameworks** (MITRE ATT&CK, NIST, PCI, HIPAA)?*
4. *How do you ensure findings are actionable and **integrated into our remediation workflows** (ticketing, SIEM, SOAR, VM tools)?*
5. *What is your overall **security posture** (SOC 2, ISO 27001, penetration testing results), and how do you handle breach notification and customer support if an incident occurs?*
6. *How do you **define and measure success** for engagements? What metrics should we expect to demonstrate risk reduction or improved resilience?*
7. *How do you support **scalability** as our organization grows or changes?*
8. *What is your **product roadmap**, and how does it align with future industry trends?*
9. *What happens if we decide to **offboard** — how will you ensure data is securely transferred or destroyed without disrupting our security program?*
10. *How transparent is your **testing methodology** (reporting detail, attack paths, toolsets) and what balance of **human expertise versus automation** is used in your approach?*

CHAPTER #8

CONCLUSION

In a market full of noise, leaders can't afford wasted budget, poor integrations, or security blind spots. The cost of the wrong decision isn't just financial but also operational risk, lost time, and eroded trust.

But procurement, done right, becomes one of the most powerful leadership tools in cybersecurity. When you apply structure to evaluation, demand transparency from vendors, and insist on measurable outcomes, you elevate procurement from a process to a strategy. You turn every engagement into an opportunity to strengthen resilience and demonstrate return on investment.

Offensive security offers something rare in this industry: **proof**. Proof that your defenses work. Proof that your investments are paying off. Proof that your organization is getting stronger.

The leaders who extract the highest ROI from offensive security understand this. They're not just buying tests. They're building continuous, measurable validation into their security programs. They treat every engagement as a feedback loop for improvement, every finding as an opportunity to get better, and every partnership as a chance to lead with evidence.

Procurement isn't about buying more tools or running more tests. It's about building trust, enabling growth, and protecting the organization.

NEXT STEPS

You now have the framework, tools, and questions to lead the procurement process with confidence. The next step is to put them into practice and move from theory to measurable action.

Start by assessing your own current offensive security partnerships and testing cadence:

- *Are your engagements uncovering meaningful attack paths or repeating surface-level findings?*
- *Can your vendors demonstrate measurable ROI and continuous improvement?*
- *Is your testing program validating resilience or just satisfying compliance?*

Use the templates, evaluation criteria, and leadership questions in this playbook to set new standards for how your organization measures success.

Share this framework with your internal teams, challenge your current assumptions, and demand transparency and accountability from every engagement.

Because leadership in procurement isn't about buying more. It's about proving more.

ABOUT SPROCKET SECURITY

Sprocket Security helps organizations measure and improve their resilience through continuous offensive security testing.

We believe security isn't proven by policies or promises, but validated through evidence.

Our approach replaces once-a-year, point-in-time testing with ongoing, measurable validation that aligns with real business outcomes. From penetration testing to red teaming and adversary simulation, Sprocket's offensive programs deliver clear, actionable insights that show leaders exactly how their defenses perform and where to improve next.

We work with organizations that value clarity over noise, accountability over assumptions, and measurable ROI over marketing hype.

If you're ready to turn your testing into continuous validation, visit sprocketsecurity.com or connect with us to learn how our team can help your organization lead procurement with confidence and proof.