ADARMA
TOGETHER WE'VE GOT THIS

GUIDE TO CREATIVE CYBERSECURITY TESTING:

Strengthen Resilience by Thinking Like an Attacker

By Leanne Salisbury, Principal Consultant at Adarma

What is Creative Cybersecurity Testing?

Creative cybersecurity testing is a way of designing scenarios that go beyond routine compliance. It's about pushing boundaries to identify hidden weaknesses, challenge assumptions, and map realistic threats to business-critical functions.

It applies to red teaming, tabletop exercises, threat modelling and crisis simulations, but the key is aligning each test with business impact, not just technical vulnerabilities.

Where Traditional Testing Falls Short

Many organisations treat testing as a checkbox exercise for auditors or regulators. This limits the scope of the test and focuses only on validating what's already known.

Creative testing flips that. It focuses on:

- What could go wrong - not just what already has
- The parts of the business that would hurt most if disrupted
- The underlying systems and services that enable revenue generation

For example:

- A retail bank might need to protect ATMs, online banking, and SWIFT
- A luxury goods firm might focus on design IP and point-of-sale systems

The goal is to expose blind spots, not just confirm defences.

Think Like an Attacker

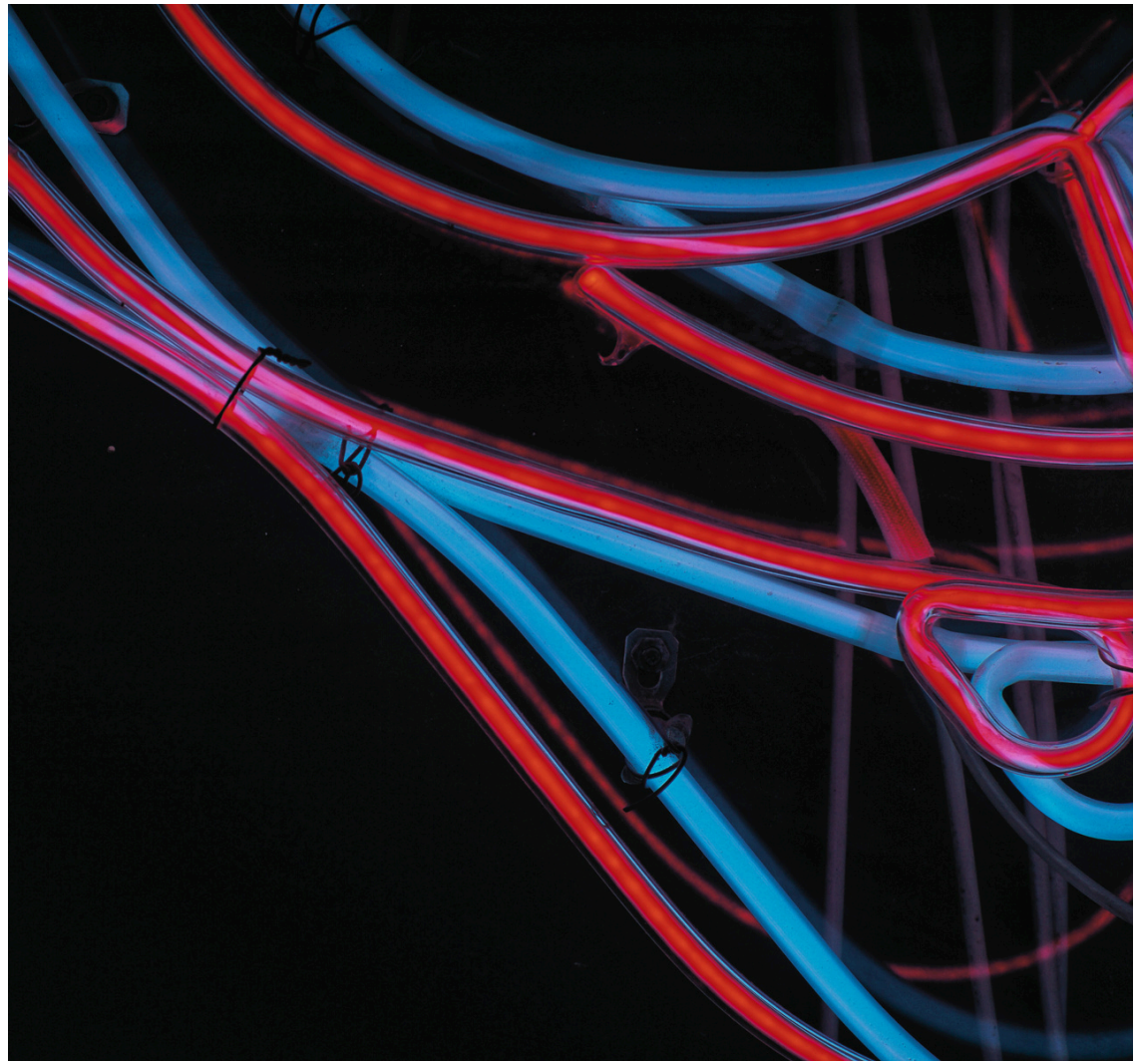
ADARMA
TOGETHER WE'VE GOT THIS

Attackers aren't abstract concepts, they're people. And they follow objectives.

Whether it's stealing data, exfiltrating funds, making a political statement, or causing disruption, they target what matters most. Creative testing adopts this mindset:

- **Identify the attacker's most likely goal**
- **Map the easiest route they might take**
- **Focus on the business impact they want to achieve**

This can be applied to red team scenarios, tabletop exercises and threat modelling. It also helps organisations step outside of their comfort zone and move beyond the idea that "we already know how the ways we might be targeted" or "I don't think that scenario will happen".



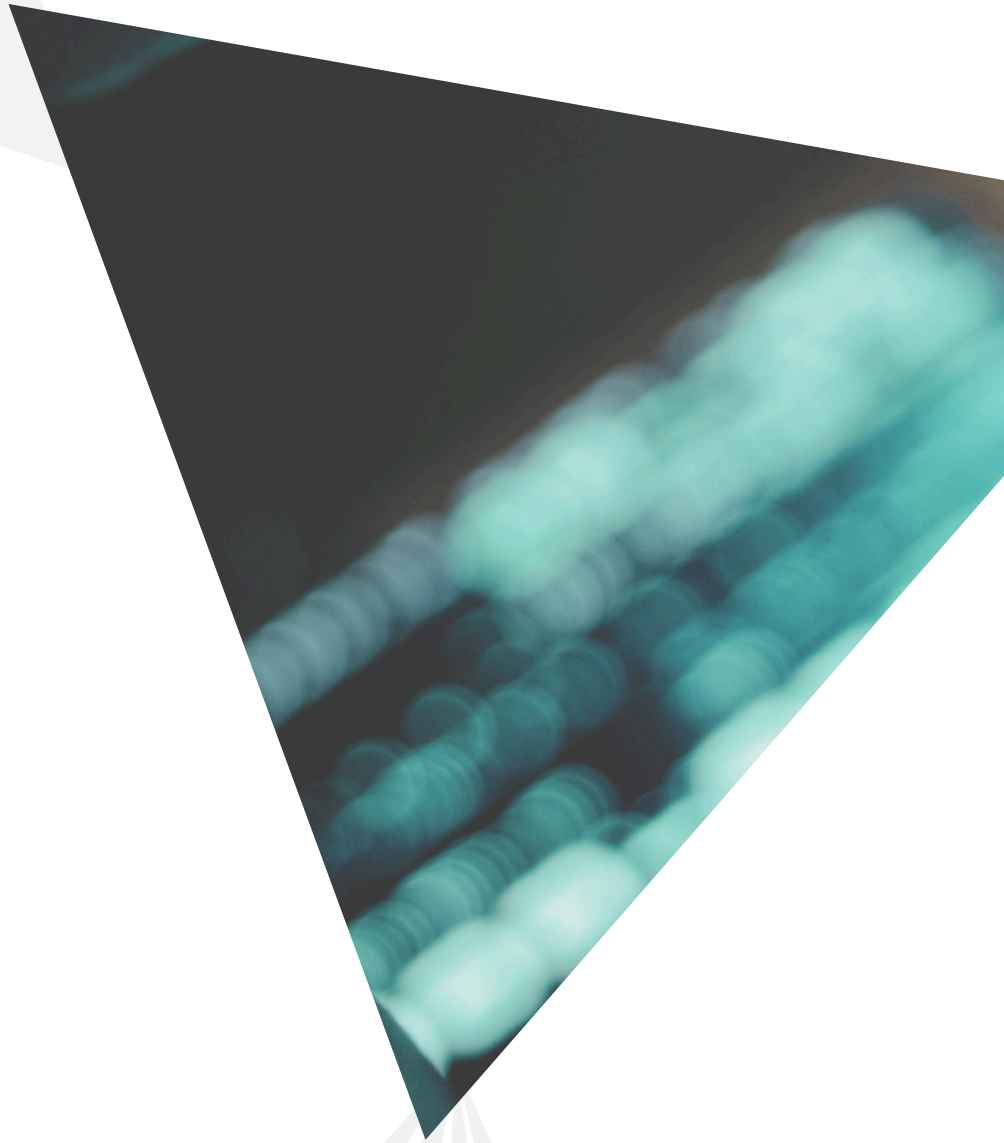
The Power of Wild Card Scenarios

Creative testing often involves wild card scenarios, events that are unlikely but potentially devastating.

The fact that many regulators mandate a requirement for these wild card scenarios in red team plans recognises their value in:

- Stress-testing security teams
- Challenging fixed assumptions
- Exposing complacency

Standard expected scenarios tend to reflect only well-understood threats. They may reassure stakeholders, but don't always build true resilience. Wild cards force teams to think on their feet and consider the unexpected.



What About Operational Technology?

Live testing in Operational Technology (OT) environments can carry serious risks. However, creative scenario development allows OT-heavy organisations to explore threats without impacting availability.

They can test:

- Hybrid attacks (combining cyber and physical elements)
- Real-world consequences such as risk to life or public safety
- Incident response and escalation protocols without touching production systems

This approach is especially valuable for Critical National Infrastructure, which can have devastating consequences of disrupted.

Understanding Who Might Target You

ADARMA
TOGETHER WE'VE GOT THIS

Creative testing starts with identifying the most relevant threat actors. Consider:

- Who targets your sector or geography?
- What are your most critical functions or data types?
- Is it availability, integrity, or confidentiality that matters most?

Think beyond the obvious:

- Motivation might be geopolitical, financial, or ideological
- Insider threats and increased media visibility can raise your risk
- Criminal ecosystems now include access brokers and Ransomware-as-a-Service
- Tools like large language models and artificial intelligence have lowered the technical barrier for attackers – so even opportunists can now pose a threat.

Breaking the “It Won’t Happen” Mindset

Just because it hasn’t happened before doesn’t mean it won’t. Mature dashboards and green KPIs are not the same as being prepared. Security is dynamic, which is why scenario testing must reflect that.

From Testing to Action

Once testing is complete, the real work begins. Don’t leave creative scenarios on paper.

Turn them into:

- A roadmap for change
- Clear actions assigned to accountable stakeholders
- Use cases in your SIEM for detection and monitoring
- Threat intelligence tasks to monitor actor behaviour or capability shifts

This approach makes security improvements measurable and justifiable to senior leadership.

What If Your Team Lacks Capacity?

You don’t need to do it all in-house.

Creative testing thrives on diverse input, technical teams, business stakeholders, threat analysts. If your team is already stretched, collaborate across departments or bring in external support. A trusted partner can help develop, facilitate, and analyse bespoke scenarios that align with your business risks.

Final Thought

Security is never static. Testing should never be routine.

Creative testing helps organisations stay sharp, challenge assumptions, and prepare for the unexpected — because in cybersecurity, it’s rarely the expected that gets you.

For more insights or support with creative cybersecurity testing, contact hello@adarma.com or visit www.adarma.com.

Get in touch

If you would like to speak to an Adarma consultant about any issue, please contact us at **hello@adarma.com**.

ADARMA

TOGETHER WE'VE GOT THIS

hello@adarma .com

www.adarma.com