

Quick Match: What Does the Customer Need?

External Vuln Assessment

"We need to know what's exposed"

- > First security initiative
- > Compliance checkbox needed
- > Small IT team / no security staff
- > Budget under \$5K/month
- > Cyber insurance requirement

PTaaS

"We need to find security holes"

- > Building/updating applications
- > Frequent code deployments
- > Need deeper than scanning
- > Compliance requires pentesting
- > Testing apps, APIs, or cloud

Red Team

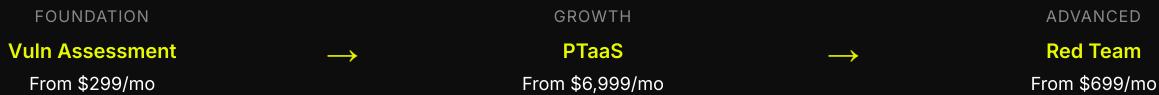
"Can we detect real attacks?"

- > Already have mature pentest program
- > EDR/XDR/SIEM deployed
- > Have SOC team or MSSP
- > Board wants assurance
- > Test human element

Pricing at a Glance

Service	Entry Price	Mid-Tier	Enterprise	Best For
Vuln Assessment	\$299/mo	\$899/mo	Custom	SMBs, compliance, continuous monitoring
PTaaS	\$6,999/mo	\$13,999/mo	\$19,999+/mo	SaaS, dev teams, deep testing
Red Team	\$699/mo	\$9,999/engagement	Custom	Mature orgs, SOC validation

Security Maturity Progression (Land & Expand)



Service Selection Objections

"We just need a pentest, not ongoing service"

Point-in-time tests create blind spots. But if budget is tight, **start with Vuln Assessment** for continuous coverage at \$299/mo, then add PTaaS when ready.

"Red teaming sounds like overkill!"

If you don't have EDR/SIEM or a SOC, you're right—**start with PTaaS**. Red team tests your ability to detect, which requires detection tools first.

"Can't we just do vuln scanning ourselves?"

You can run scans, but you'll drown in **false positives (up to 80%)**. Our analysts validate everything. How much is your team's time worth triaging noise?

"PTaaS is too expensive for us"

Compare to one-off pentests (\$15-50K each) or hiring (\$150K+/year). If truly budget-constrained, **Vuln Assessment** gives continuous coverage at \$299/mo.

"We need all three—can we get a discount?"

Absolutely. **Bundle pricing available**—let's scope your environment and I'll put together a custom package. Multi-service clients get priority support too.

Discovery Questions

- ? What's driving this security initiative? (Compliance, incident, board pressure?)
- ? Do you have a security team, or is IT handling security?
- ? What security tools do you have deployed? (EDR, SIEM, scanners?)
- ? How often do you release new code or make infrastructure changes?
- ? Have you done pentesting before? How did it go?
- ? What compliance frameworks apply? (SOC 2, PCI, HIPAA, etc.)
- ? What's your approximate security budget?
- ? Who needs to approve this decision?

Bundle Opportunities

Common Service Combinations

Vuln Assessment + PTaaS	Continuous external + deep app testing
PTaaS + Red Team	Find vulns + test detection
All Three Services	Complete security validation program

Upsell & Cross-Sell Triggers

Vuln Assessment → PTaaS

When they say:

Vuln Assessment → Red Team

When they say:

PTaaS → Red Team

When they say:

"We found web app vulnerabilities" or "We're launching a new product" or "Auditor wants manual testing"

"External scan is clean" or "We deployed EDR" or "Board wants breach simulation"

"We fixed everything you found" or "We built a SOC" or "We want to test our people"

Red Team → PTaaS

When they say:

"We found gaps in our apps" or "We need continuous testing" or "New dev team hired"

PTaaS → Vuln Assessment

When they say:

"We want continuous monitoring" or "Insurance requires monthly scans" or "Budget for ongoing"

Any → Bundle

When they say:

"We need comprehensive coverage" or "What else should we do?" or "Board wants full program"

Wrong Service Signals

- ! Wants Red Team but no security tools → Point to PTaaS or Vuln Assessment first
- ! Wants PTaaS but only has 2 public IPs → Vuln Assessment is better fit
- ! Wants Vuln Assessment but needs app testing → PTaaS is the right choice
- ! Budget under \$200/mo → May not be ready; suggest free consultation
- ! Expects one service to solve everything → Educate on layered approach

Quick Pitch by Persona

CEO/CFO: "Predictable cost, compliance coverage, risk reduction"

CTO/VP Eng: "Test as you ship, real findings, no false positives"

CISO/Security: "Validate controls, MITRE coverage, executive reporting"

Compliance: "Audit-ready reports, framework mapping, evidence"