ThreatMate Battlecards for Pax8

In-catalog: ConnectSecure

Quick positioning
ThreatMate helps MSPs productize weekly/ongoing pentesting, then consolidate surrounding security tools into one platform. Instead of endless vulnerability lists, MSPs get validated, exploitable findings and client-ready proof across external exposure, Microsoft 365 posture, identity risk, and dark web monitoring.

When to lead with ThreatMate

- They already scan for vulnerabilities, but clients are asking for pentesting and proof.
- They use multiple tools (pentest + assessments + posture) and want to consolidate.
- They struggle with alert overload and manual report stitching for QBRs and prospects.

Fast qualify

Do they already have vulnerability scanning or posture tools in place?

YES Pentesting motion: add ongoing pentesting and client-ready proof.

NO Consolidation motion: replace point tools with one platform.

ThreatMate vs ConnectSecure

IN-CATALOG

Best fit
Using ConnectSecure (or similar) for vulnerability + compliance, but customers are now asking for pentesting and validation.

Say this
ConnectSecure helps manage vulnerabilities and compliance. ThreatMate adds ongoing pentesting and shows what is actually exploitable, with proof you can use in QBRs and sales conversations.

Ask
Are you mainly managing vulnerabilities today, or are you trying to sell recurring pentesting with proof of risk reduction?

ThreatMate adds
• Weekly/ongoing automated pentesting across tenants.
• Validated priorities so techs know what actually matters.
• External exposure, Microsoft 365 posture, identity risk, and dark web monitoring.
• Client-ready reporting for prospecting, QBRs, and renewals.

ThreatMate Battlecards for Pax8

In-catalog: Augmentt

Quick positioning
ThreatMate helps MSPs productize weekly/ongoing pentesting, then consolidate surrounding security tools into one platform. Instead of endless vulnerability lists, MSPs get validated, exploitable findings and client-ready proof across external exposure, Microsoft 365 posture, identity risk, and dark web monitoring.

When to lead with ThreatMate

- They already scan for vulnerabilities, but clients are asking for pentesting and proof.
- They use multiple tools (pentest + assessments + posture) and want to consolidate.
- They struggle with alert overload and manual report stitching for QBRs and prospects.

Fast qualify

Do they already have vulnerability scanning or posture tools in place?

YES Pentesting motion: add ongoing pentesting and client-ready proof.

NO Consolidation motion: replace point tools with one platform.

ThreatMate vs Augmentt

IN-CATALOG

Best fit
Using Augmentt to standardize Microsoft 365 security, but still need pentesting and external validation to tell a complete risk story.

Say this
Augmentt is strong for Microsoft 365 posture. ThreatMate layers on ongoing pentesting and validation across the rest of the attack surface, then turns it into client-ready proof.

Ask
Is Microsoft 365 posture enough, or do you also want recurring pentesting with proof you can sell?

ThreatMate adds
• Weekly/ongoing pentesting beyond M365.
• Validation of exploitable paths, not just configuration scores.
• Unified view across external, M365, identity risk, and dark web.
• Sales and QBR-ready reporting.

ThreatMate Battlecards for Pax8

Off-catalog redirects

Vonahi

REDIRECT

Best fit
Automated network pentesting (often sold as per-test).

Say this
ThreatMate adds weekly/ongoing cadence plus consolidation of posture and assessment tools into one platform.

Ask
Are you looking for a single pentest tool, or a recurring pentesting program with proof across the full attack surface?

Nodeware

REDIRECT

Best fit
Continuous vulnerability scanning focused on detection.

Say this
ThreatMate validates what's exploitable and tracks improvement over time so you can prove value in QBRs.

Ask
When you find vulns, how do you prove what mattered and what improved month over month?

Cavelo

REDIRECT

Best fit
Attack surface visibility and mapping.

Say this
ThreatMate adds pentesting validation and prioritized remediation so visibility turns into outcomes and proof.

Ask
Do you want visibility, or validated proof you can sell and review in QBRs?

Galactic Advisors

REDIRECT

Best fit
Services-heavy pentesting engagements (high-touch, harder to scale).

Say this
ThreatMate productizes pentesting weekly across all customers so MSPs can deliver it profitably at scale.

Ask
Is this a one-time services engagement, or do you need a scalable recurring program?

Tip: If the MSP is trying to productize weekly pentesting or consolidate tools, lead with ThreatMate.

ThreatMate Battlecards for Pax8

Off-catalog + opener

RapidFire

REDIRECT

Best fit
Assessment-based reporting and network data collection.

Say this
ThreatMate adds continuous pentesting and validated risk, then turns it into client-ready proof for renewals.

Ask
Are you delivering a one-time assessment report, or an ongoing security program with proof?

10-second opener
Already scanning but clients want pentesting proof? ThreatMate productizes weekly pentesting and consolidates surrounding tools, so MSPs get validated priorities and client-ready proof without alert overload.