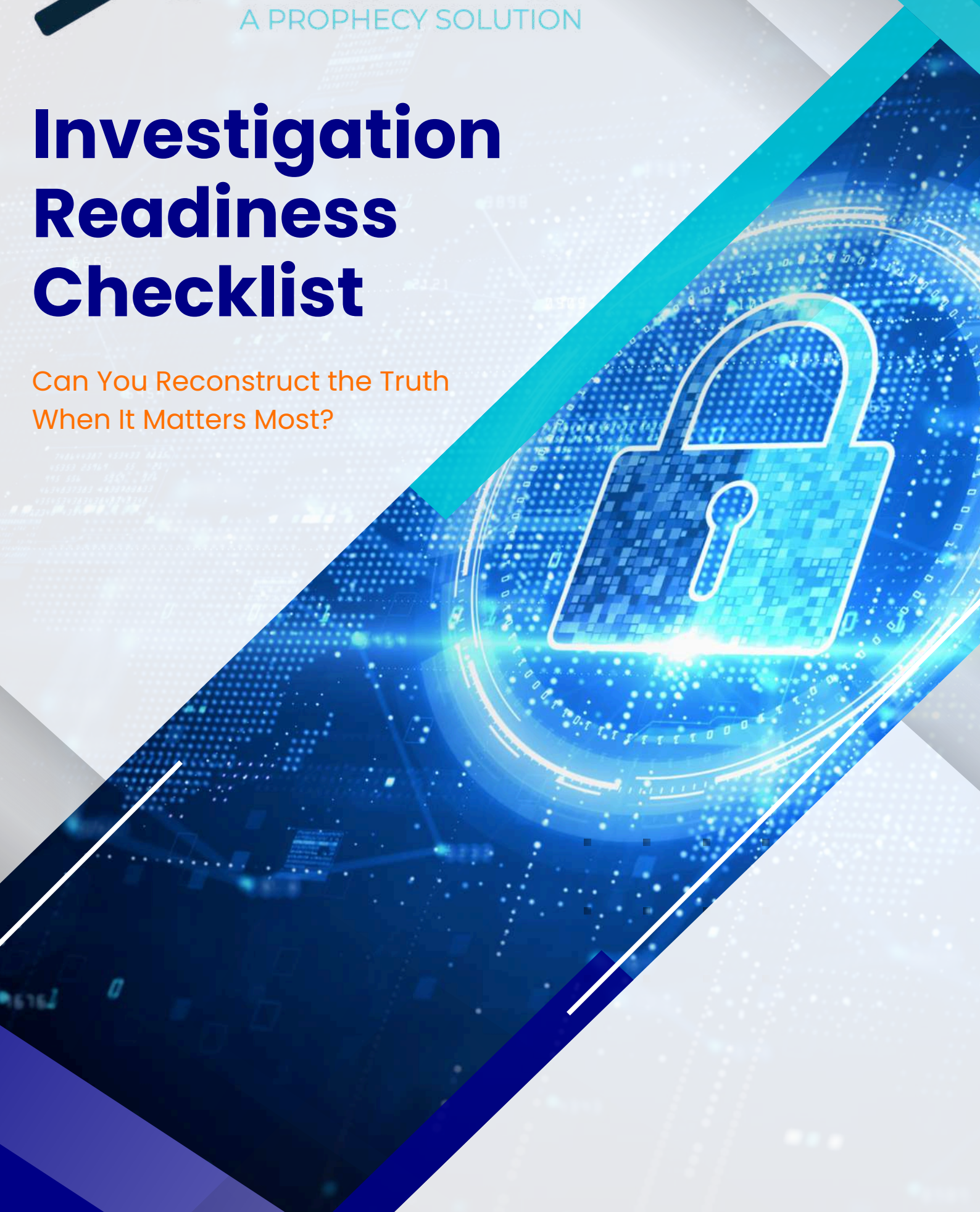
snare
A PROPHECY SOLUTION

Investigation Readiness Checklist

Can You Reconstruct the Truth When It Matters Most?



Readiness Is Not About Detection

Most organisations measure security maturity by:

- Number of alerts
- Speed of detection
- Coverage of tools

But when a real incident occurs, those metrics become secondary.

The real question becomes:

Can you reconstruct what actually happened — quickly, confidently, and completely?

According to Gartner, organisations are increasingly shifting from prevention-focused models to investigation and response maturity, as attackers bypass traditional controls.

What Makes This Checklist Different

This is not a list of controls.

This is a test of your **ability to answer critical questions under pressure.**

THE MOMENT OF TRUTH

Imagine this scenario:

A potential breach is detected.
You are asked:

- What happened?
- When did it start?
- What systems were affected?
- What data was accessed?
- Is it contained?

The Reality

Most organisations cannot answer these questions within the first 24 hours.

Your First Test

Can you answer these within 15 minutes?

- Where did the initial access occur?
- Which identity was used?
- What was the first action taken?

Scoring

- **Yes, immediately** → High readiness
- **With effort** → Moderate readiness
- **Not confidently** → Critical gap

IDENTITY → ACTIVITY → IMPACT

Investigation is not about isolated events.

It is about **connecting a chain of truth.**

Test 2: Can You Link Identity to Activity?

- Can you trace a user from login → to actions → to outcomes?
- Can you identify privilege escalation during a session?
- Can you detect behaviour that deviates from role expectations?

Test 3: Can You Track Movement Across Systems?

- Can you follow activity across endpoints, cloud, and applications?
- Can you track lateral movement without relying on alerts?
- Can you correlate events across multiple environments?

Test 4: Can You Prove Impact?

- Can you identify what data was accessed or moved?
- Can you confirm what was changed or deleted?
- Can you validate whether exfiltration occurred?

If you cannot connect identity → activity → impact,
you cannot complete an investigation.

TIME — YOUR BIGGEST ENEMY

Most investigations fail not because of missing tools — but because of missing time.

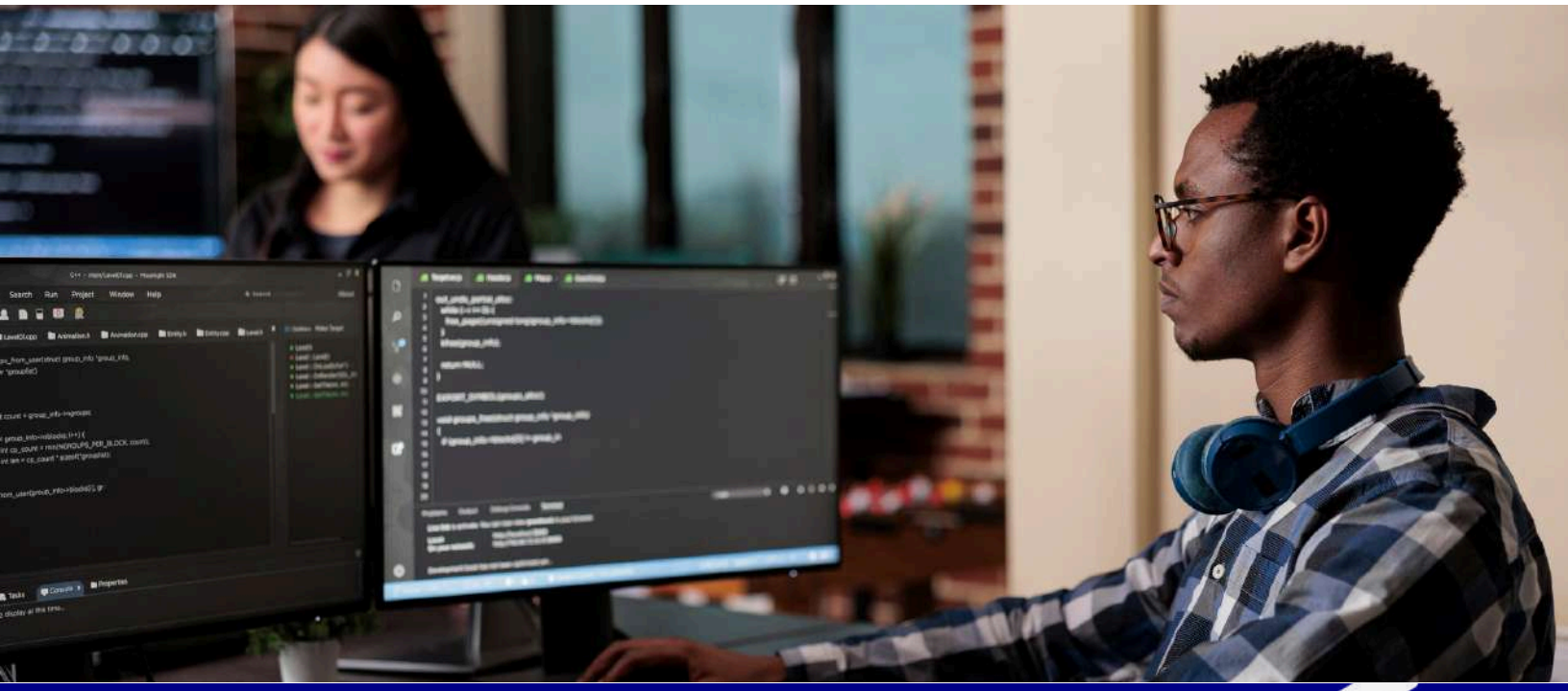
Test 5: Do You Have Enough History?

- Are logs retained long enough to investigate delayed detection?
- Can you access historical data without rehydration delays?
- Can you compare behaviour over time?

Test 6: Can You Rewind and Replay?

- Can you reconstruct past events in sequence?
- Can you replay logs to identify missed signals?
- Can you validate assumptions with historical evidence?

If your data is gone, your investigation stops.



SIGNAL VS NOISE

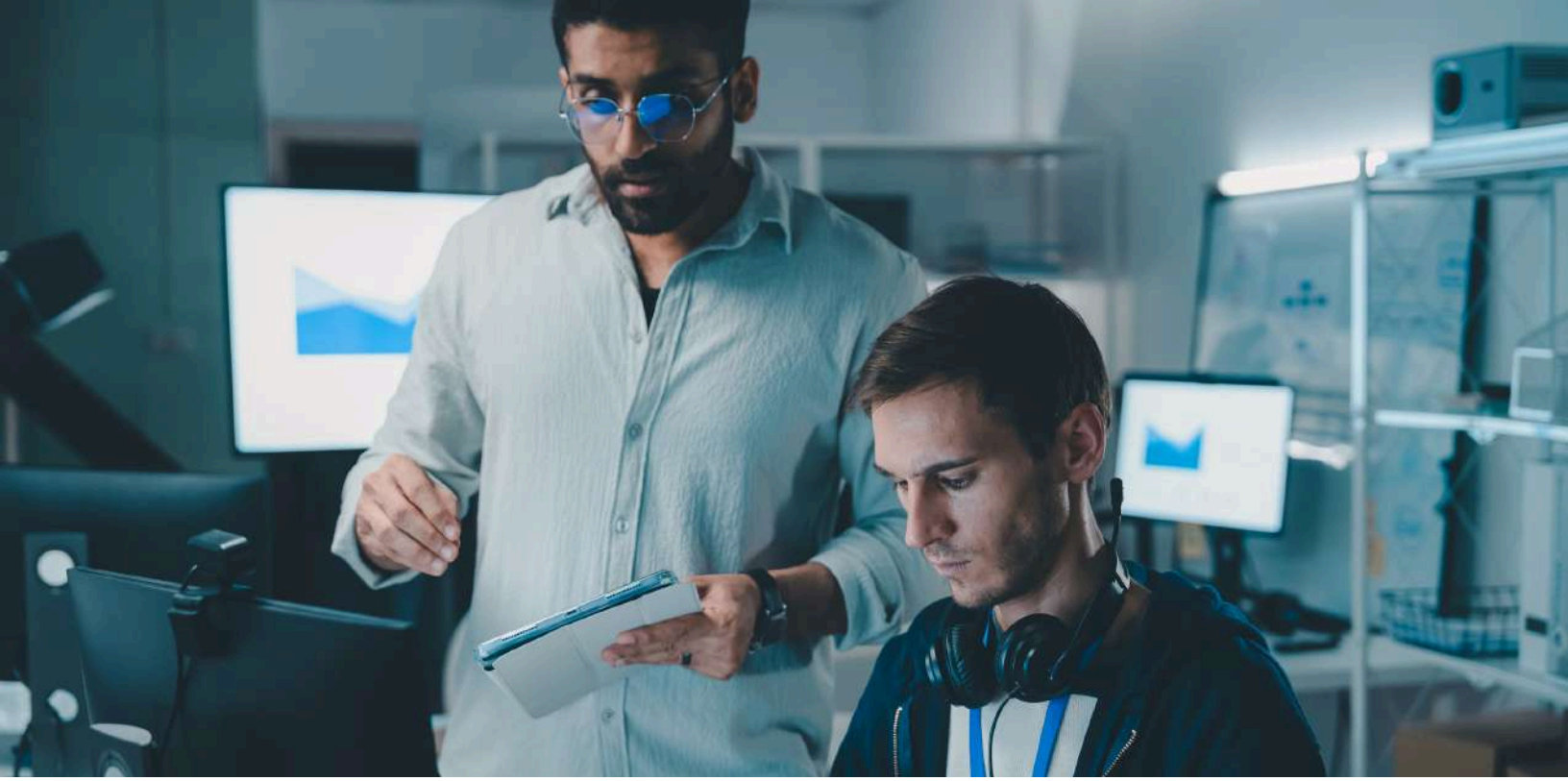
Modern environments generate enormous volumes of data.
But more data does not equal more clarity.

Test 7: Can You Reduce Noise Without Losing Truth?

- Are you filtering data before understanding its value?
- Can you separate meaningful activity from background noise?
- Can you refine investigations without losing fidelity?

According to Gartner, alert fatigue and data overload are among the top challenges for SOC teams.

If everything looks important, nothing is.



INVESTIGATION SPEED

Speed is not about dashboards.

It is about how quickly you can build a narrative.

Test 8: How Long Does It Take to Answer These?

- What happened?
- Who was involved?
- What systems were affected?
- What is the scope of impact?

Scoring Guide

- **Minutes** → Investigation-ready
- **Hours** → Operationally strained
- **Days or unknown** → High risk

THE CONFIDENCE TEST

Even if you can answer the questions...

Test 9: Can You Defend Your Findings?

- Are your conclusions backed by verifiable logs?
- Can you prove timelines and actions with evidence?
- Would your investigation stand up to audit or legal review?

Confidence without evidence is risk.

FINAL SCORECARD

Count your results across all tests:

HIGH READINESS

- You can reconstruct incidents quickly
- You have strong visibility and traceability
- Your investigations are defensible

MODERATE READINESS

- You can answer some questions
- Gaps exist in correlation or retention
- Investigations take time and effort

LOW READINESS

- You rely heavily on alerts
- You lack visibility across systems
- You cannot confidently prove impact

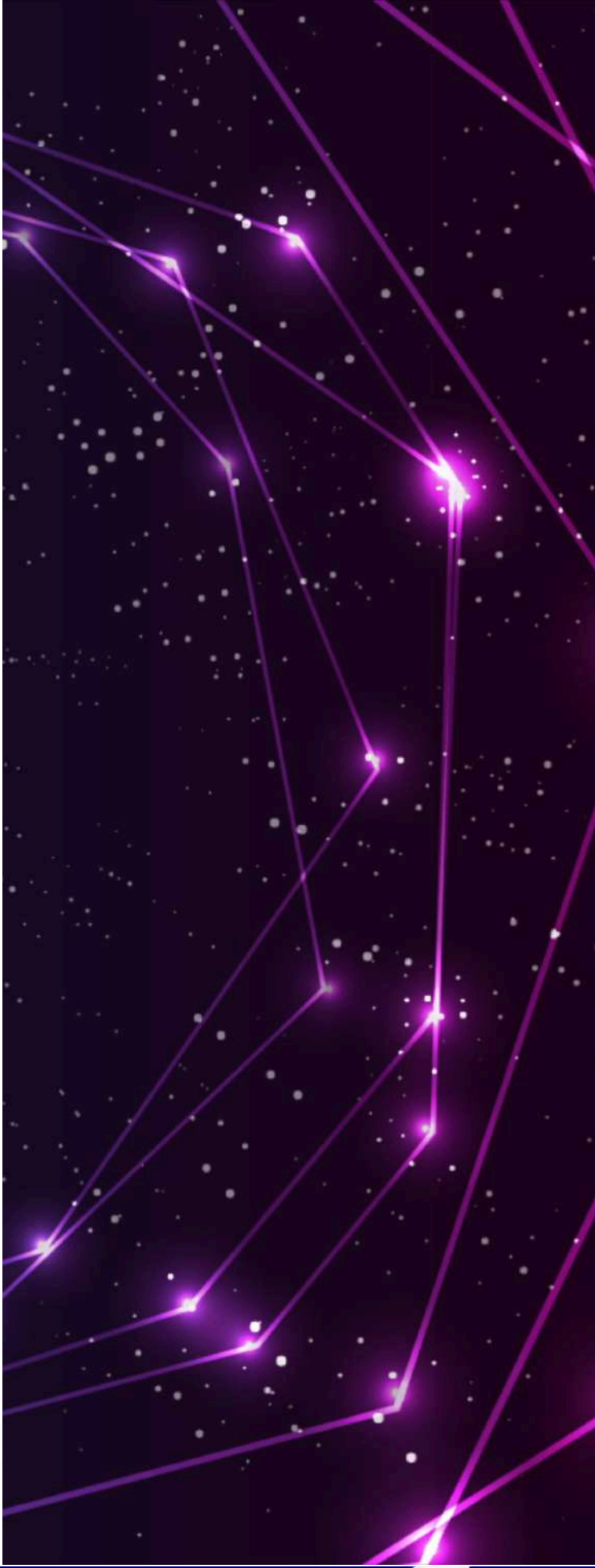
WHAT TO DO NEXT

Investigation readiness is not achieved by adding more tools.

It requires:

- Better visibility across systems
- Stronger linkage between identity and activity
- Retention of high-fidelity log data
- Ability to reconstruct events over time

The goal is not to detect everything.
It is to understand anything.



Are You Truly Investigation Ready?

Most organisations aren't — until it's too late.

Take the Next Step

- Identify your investigation gaps
- Benchmark your readiness
- Build a defensible logging strategy

Book a Log Strategy Session

Need a foundation first?
→ Download: MSSP Logging Baseline Template
(Standardise visibility before improving investigations)

snare
A PROPHECY SOLUTION

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

snare
A PROPHECY SOLUTION