Is Your Tool Stack Really Protecting You?

Score each statement honestly. This isn't a test, it's a map of where your risks are hiding.

CYBERLEAF | Ontech SYSTEMS, INC.

How to score: For each statement, circle the number that best reflects your organization today. Total each category, then flip to the back to interpret your results and get a realistic first action plan.

Scoring Key: 0 Not in place / don't know 1 Partially in place / inconsistent 2 Fully in place / confident

1 Ownership & Accountability

Every security tool in our environment has a named owner responsible for monitoring it.	0	1	2
We have a documented process for who responds to alerts — and that process is actually followed.	0	1	2
Our executives can explain what outcomes our security stack is designed to achieve.	0	1	2
Third-party vendors with network access are tracked and held to defined security standards.	0	1	2

Categopry Total: _/8

2 Tool Integration & Visibility

Our security tools share data with each other — alerts from one inform another.	0	1	2
We have a single pane of glass (or close to it) for reviewing security status across the environment.	0	1	2
We can correlate an alert from endpoint protection with identity and network data quickly.	0	1	2
We know whether each tool is configured to its full capability — not just installed.	0	1	2

Categopry Total: _/8

3 Defense in Depth

We have defined controls across all four phases: prevention, detection, response, and recovery.	0	1	2
Identity protection (MFA, privileged access) is treated as the highest priority control layer.	0	1	2
We have tested our incident response plan in the last 12 months — not just documented it.	0	1	2
Our backups have been verified — we know how fast we can recover and have tested it.	0	1	2

Categopry Total: _/8

4 Risk Awareness & Strategy

We maintain a risk register — risks are documented, prioritized, and reviewed regularly.	0	1	2
When we accept a risk, that decision is deliberate and documented — not just overlooked.	0	1	2
We can measure and report security improvement over time with concrete metrics.	0	1	2
We have a written security roadmap — a forward-looking strategy, not just a list of tools.	0	1	2

Categopry Total: _/8

Add your four category totals for your Overall Score (max 32). • Write it here: _____ / 32 FLIP OVER TO INTERPRET YOUR SCORE →

Your Score. Your Next Move.

Use your total from the front to find where you stand — and what to do first.

0 - 12
High Exposure

Significant gaps in ownership, visibility, or strategy. A single incident could have serious operational impact. Start with a security assessment now.

13 - 22
Partial Coverage

Some controls exist but they're inconsistent or siloed. You're likely missing integration between tools and clarity on who owns what. A gap analysis will surface quick wins.

23 - 32
Strong Foundation

Your fundamentals are solid. Focus now shifts to optimization, tabletop exercises, and ensuring your roadmap is keeping pace with evolving threats, especially AI-accelerated attacks.

If you scored 0-12: Start with a Security Assessment

- [ ] Inventory every tool in your environment — who bought it, when, and what it's supposed to do.
- [ ] Identify who owns each tool. If the answer is "nobody" or "everyone," that's your first fix.
- [ ] Request a free attack surface map from OnTech — it will show you what's exposed right now.
- [ ] Don't buy anything new yet. The problem is almost never missing tools — it's how existing ones are used.

If you scored 13-22: Close the Integration Gaps

- [ ] Run a gap analysis using the Cyber Defense Matrix — map your tools against the five functions (Identify, Protect, Detect, Respond, Recover).
- [ ] Connect your endpoint and identity tools. Most environments have both — very few have them talking to each other.
- [ ] Build a risk register. Even a simple spreadsheet that executives review quarterly changes the conversation dramatically.
- [ ] Schedule a tabletop exercise — walk leadership through a ransomware scenario to get budget and buy-in aligned with actual risk.

If you scored 23-32: Optimize & Pressure Test

- [ ] Review your mean time to detect, respond, and recover. If you're not tracking these, start; they're your real security KPIs.
- [ ] Simulate a real attack scenario against your current environment. Find the weakest link and then fix that one path before moving on.
- [ ] Review your AI-use policy. If you don't have one, your staff is already making their own rules around what's allowed.
- [ ] Consider whether your managed security partner is providing quarterly risk briefings. If they're not, ask why not.

In the Defense Industrial Base? Add This Lens.

- [ ] CMMC compliance is now tied directly to contract eligibility. If any portion of your revenue flows from DoD contracts — even indirectly — CMMC applies to you.
- [ ] CMMC Level 1 is achievable for most organizations. Level 2 requires documented practices and, eventually, a third-party assessment.
- [ ] Cyberleaf is a CMMC L2 RPO. We can help you understand your gap, build your roadmap, and provide ongoing managed security services through a certified SOC — without a sixfigure upfront commitment.

Ready to turn this assessment into a plan? **We'll do the heavy lifting.**

Ontech Systems
sales@ontech.com

Cyberleaf
cyberleaf.io