CYBERSECURITY REALITY CHECK

A PRACTICAL SELF-ASSESSMENT FOR SECURITY PROGRAM MATURITY

Security maturity is not what you believe to be true,
it is what holds up under pressure.

Created By: Daniel Gregory | Astro
dgregory@astrodefend.com

Creation Date: March, 2026
Version: v1.0

PURPOSE

This document is designed to provide a simple, honest, and practical way to evaluate the effectiveness of your organization's cybersecurity program.

This is **not an audit** and not intended for compliance purposes.

It is a **working exercise** meant to help leadership and security teams:

- Identify gaps in foundational capabilities
- Align on actual (not perceived) maturity
- Prioritize actions that meaningfully reduce risk

This assessment is most effective when completed collaboratively across security, IT, and business leadership.

INSTRUCTIONS

For each question, answer using one of the following:

- **Yes** – Consistently true across the organization
- **No** – Not true or inconsistently applied
- **Unsure** – Lack of clarity or confidence

Be objective. The value of this exercise depends entirely on honest answers.

SECTION 1 - FUNDAMENTALS

1. Do we have a complete and continuously updated inventory of all assets (on-prem, cloud, SaaS)?
2. Are critical vulnerabilities consistently remediated within defined SLAs?
3. Do we have consistent logging and visibility across all critical systems?

SECTION 2 - TOOLING VS. OPERATIONS

1. Are all major security tools fully configured, integrated, and actively used?
2. Do we routinely validate that alerts are investigated and acted upon?
3. Have we rationalized overlapping or redundant tools in the last 12–18 months?

SECTION 3 - MATURITY

1. Have we tested our incident response capability in a realistic scenario in the last 12 months?
2. Do we measure actual performance (e.g., detection and response times), not just control presence?
3. Would our response hold up under real-world pressure today?

SECTION 4 - PRIORITIES

1. Are we prioritizing remediation based on real risk, not trends or new technologies?
2. Are known, high-probability risks fully addressed before investing in advanced capabilities?
3. Can we clearly justify how current investments reduce material risk?

SECTION 5 - OPERATIONS

1. Is ownership of security risks clearly defined across the organization?
2. Are security processes consistently executed, not just documented?
3. Do teams know exactly what to do during a real incident?

INTERPRETING YOUR RESULTS

- **5 or more "No / Unsure" responses** - Likely indicates systemic gaps in the program
- **8 or more "No / Unsure" responses -** Indicates limited operational resilience
- **10 or more "No / Unsure" responses -** Suggests maturity is being significantly overestimated

RECOMMENDED NEXT STEP

Review each "No" or "Unsure" response with your team and:

- Identify root causes (process, ownership, tooling, or capability)
- Prioritize based on risk and business impact
- Establish clear ownership and timelines for remediation

This exercise is most valuable when used as a starting point for focused, practical improvement, not as a one-time assessment.