5 Fast Wins for New CISOs:
A Tactical Checklist to Build Credibility Fast

When you're a new CISO, early traction matters. You're inheriting a complex environment, managing executive expectations, and working against the clock. These five wins are designed to help you quickly establish control, reduce real risk, and prove value in business terms.

1. VALIDATE AND PRIORITIZE YOUR ASSET INVENTORY

WHY IT MATTERS:
Visibility gaps = risk blind spots. Before you can defend, you need to know what you're protecting.

ACTIONS:
- Audit your asset inventory—assume your CMDB is ~60% accurate at best.
- Identify unmanaged devices, legacy infrastructure, and cloud workloads.
- Prioritize assets by business impact (customer-facing apps, finance systems, regulated data).

QUICK WIN METRIC: % increase in verified crown-jewel asset coverage

2. EXPAND AND MAP TELEMETRY COVERAGE

WHY IT MATTERS:
You can't detect or respond to what you can't see.

ACTIONS:
- Validate log sources across identity, cloud, endpoint, and network.
- Map telemetry coverage to your SIEM or MDR platform—where are the gaps?
- Run a simulated lateral movement or identity-based attack—can you trace the full path?

QUICK WIN METRIC: # of new log sources onboarded + % telemetry coverage on high-risk assets

3. REDUCE ALERT FATIGUE AND FOCUS ON WHAT MATTERS

WHY IT MATTERS:
Inherited noise clogs workflows, wastes analyst time, and hides real threats.

ACTIONS:
- Identify the top 10 noisiest detection rules—tune or suppress as needed.
- Apply business context to alerting: crown-jewel systems get elevated, low-value assets get deprioritized.
- Launch a suppression sprint with SOC or MDR partners to eliminate false positives.

QUICK WIN METRIC: % reduction in low-fidelity alerts + ratio of actionable to total alerts

4. FIX OR CONTAIN CRITICAL VULNERABILITIES

WHY IT MATTERS:
Demonstrating a measurable reduction in exploitable risk builds immediate trust.

ACTIONS:
- Prioritize patching for actively exploited or high-impact CVEs (especially on internet-facing assets).
- Where patching isn't possible, apply compensating controls: isolation, stricter logging, firewall tuning.
- Use threat intelligence to prioritize by exploitability, not just CVSS scores.

QUICK WIN METRIC: # of critical vulnerabilities remediated or mitigated within 30 days

5. DELIVER A 30-DAY EXECUTIVE SCORECARD

WHY IT MATTERS:
CISOs don't just fix things—they frame security as a business enabler.

ACTIONS:
- Package before/after metrics into a clean, visual report for execs.
- Align outcomes to business priorities: reduced downtime risk, faster incident response, improved audit posture.
- Include a roadmap preview—what you've learned, where you're going, and what support you'll need.

QUICK WIN METRIC: On-time delivery of scorecard + executive feedback or sponsorship earned

FINAL NOTE:

You don't need new tools or headcount to create momentum. These wins can be delivered using what's already in place—faster if you leverage an MDR partner like Deepwatch to operationalize your first 100 days.

GET STARTED