YUDU Sentinel
Your Crisis Response Toolbox

MSSP Security Assurance Scorecard

A practical assessment tool to identify whether your MSSP is strengthening or weakening your cyber security posture.

Scoring:
1 = Very weak
2 = Needs improvement
3 = Adequate
4 = Strong
5 = Excellent / Best practice

1. RESILIENCE & SINGLE POINT OF FAILURE	SCORE	BASIS FOR SCORE
How resilient is your security if the MSSP itself goes down?		
• Redundant, geographically separated SOCs		
• Operational failover tested and proven		
• Clear plan for MSSP outage or breach		
• Clear fallback approach if MSSP becomes unavailable		
• Secure Out-of-Band Communications Platform in place for continuity		
Average Score		
2. PRIVILAGED ACCESS MANAGEMENT	**SCORE**	**BASIS FOR SCORE**
Does the MSSP hold the “keys to the kingdom” securely?		
• Least-privilege access enforced		
• Regular credential rotation		
• Segregated analyst access by client		
• Full logging & auditability of privileged actions		
• Out-of-Band escalation available if identity systems fail		
Average Score		
3. TRANSPARENCY & VISIBILITY	**SCORE**	**BASIS FOR SCORE**
Do you truly understand how your MSSP works?		
• Detection logic explainable and transparent at the methodology level		
• Alert triage workflows clearly documented		
• Detections validated regularly		
• Reports provide insight, not activity summaries		
• No “black box” tooling		
Average Score		
4. DETECTION QUALITY & THREAT COVERAGE	**SCORE**	**BASIS FOR SCORE**
Is detection tailored, current, and effective?		
• Custom rule sets aligned to your assets and threats		
• Frequent tuning and continuous updates		
• Multi-source threat intelligence		
• Regular threat modelling sessions		
• Demonstrated detection efficacy (tests, audits)		
Average Score		
5. SLA PERFORMANCE IN REALITY	**SCORE**	**BASIS FOR SCORE**
Do they respond as fast as they promise?		
• Actual response matches SLA commitments		
• Rapid escalation on high-severity alerts		
• Evidence analyst capacity meets SLA requirements		
• Clear “time to action” metrics		
• Rapid communication cycle during incidents		
Average Score		
6. COMPLIANCE VS REAL SECURITY	**SCORE**	**BASIS FOR SCORE**
Do they deliver protection or just paperwork?		
• Actionable recommendations in reports		
• Focus on reducing real attack paths		
• Evidence of measurable risk reduction		
• Support beyond monitoring (e.g., hardening, tuning)		
• Avoidance of “compliance theatre”		
Average Score		

7. INTERNAL CAPABILITY STRENGTHENING	SCORE	BASIS FOR SCORE
Is the MSSP building your competence, not replacing it?		
• Clear shared responsibility models		
• Knowledge transfer to internal teams		
• Improving internal teams ability to operate independently in outages		
• Helping internal staff to understand detection and response flows		
• Joint exercises and continual skill development		
Average Score		
8. MSSP SUPPLY CHAIN SECURITY	**SCORE**	**BASIS FOR SCORE**
Do you understand the providers behind your provider?		
• Third-party tooling fully disclosed		
• Sub-processors vetted and monitored		
• Offshore SOC locations transparent		
• MSSP can articulate and evidence its supplier risk controls		
• No hidden access paths to your data		
Average Score		
9. CLIENT SEGREGATION & CONTAINMENT	**SCORE**	**BASIS FOR SCORE**
How effectively are you isolated from other clients?		
• Clear multi-tenancy isolation guarantees		
• No shared admin accounts		
• Segregated infrastructure and pipelines		
• Controls to prevent cross-client breach propagation		
• Strong governance of analyst access boundaries		
Average Score		
10. CONTRACT COMPLETENESS & CLARITY	**SCORE**	**BASIS FOR SCORE**
Does the contract reflect real operational needs?		
• Incident response included, not optional		
• No exclusions for critical systems (cloud/OT/SaaS)		
• Root-cause investigations covered		
• Liability framework aligns with operational risk		
• Responsibilities and escalation maps clearly defined		
Average Score		
11. INCENTIVE ALIGNMENT	**SCORE**	**BASIS FOR SCORE**
Are their incentives aligned with lowering your risk?		
• No financial incentive for MSSP to increase incident/alert volumes		
• Recommendations not tied to upselling		
• Focus on long-term resilience, not alert volumes		
• Mutually beneficial success metrics		
• Incentives for reducing workload through hardening		
Average Score		
12. CRISIS RESPONSE INTEGRATION	**SCORE**	**BASIS FOR SCORE**
Can the MSSP operate with you in a true crisis?		
• Rapid joining of crisis calls		
• Out-of-Band Communications Platform integration		
• Involvement in tabletop and simulation exercises		
• Understanding of your escalation paths		
• Alignment with business continuity, not just IT response		
Average Score		
OVERALL RISK SCORE **Add your 12 category scores (max 60)**		

WHAT YOUR OVERALL SCORE MEANS

50–60: Excellent - MSSP is a strong, resilient partner
40–49: Solid - Improvements needed, but generally sound
30–39: Moderate risk - Gaps could weaken your posture
20–29: High risk - MSSP may be undermining your security
0–19: Critical risk - Immediate review recommended