InventiveHQ

Security Monitoring Gap Assessment

Is Your Business Protected When It Matters Most?

75% of cyberattacks occur outside business hours. This assessment helps you identify critical blind spots in your security monitoring that attackers exploit.

How to Use This Assessment

1. **Answer each question honestly** - Your security depends on accurate self-assessment
2. **Score your responses** using the point values provided
3. **Calculate your total score** at the end of each section
4. **Review your risk level** and recommended actions
5. **Take action** based on your identified gaps

Assessment Questions

Section A: Coverage Hours (Maximum 25 points)

A1. Do you have 24/7 security monitoring in place?

- [ ] Yes, we monitor around the clock (5 points)
- [ ] We monitor during extended hours (3 points)
- [ ] Business hours only (1 point)
- [ ] No continuous monitoring (0 points)

A2. Are weekends covered by security monitoring?

- [ ] Yes, full weekend coverage (5 points)
- [ ] Partial weekend coverage (2 points)
- [ ] No weekend coverage (0 points)

A3. Are holidays covered by security monitoring?

- [ ] Yes, all holidays covered (5 points)
- [ ] Some holidays covered (2 points)
- [ ] No holiday coverage (0 points)

A4. Can someone respond to critical security alerts within 1 hour at 2 AM?

- [ ] Yes, guaranteed response (5 points)
- [ ] Sometimes, depends on availability (2 points)
- [ ] No after-hours response capability (0 points)

A5. Do you have documented after-hours escalation procedures?

- [ ] Yes, tested and current (5 points)
- [ ] Yes, but outdated (2 points)
- [ ] No escalation procedures (0 points)

Section A Score: _____ / 25

Section B: Alert Management (Maximum 25 points)

B1. How many security alerts do you receive daily?

- [ ] Manageable amount, all reviewed (<100) (5 points)
- [ ] Moderate volume (100-500) (3 points)
- [ ] Overwhelming volume (500+) (1 point)
- [ ] Don't track alerts (0 points)

B2. What percentage of security alerts are investigated?

- [ ] 100% investigated (5 points)
- [ ] 75-99% investigated (3 points)
- [ ] 50-74% investigated (1 point)
- [ ] Less than 50% or unknown (0 points)

B3. Do you have automated alert triage and prioritization?

- [ ] Yes, fully automated (5 points)
- [ ] Partially automated (3 points)
- [ ] Manual process only (1 point)
- [ ] No triage process (0 points)

B4. Can your team quickly distinguish false positives from real threats?

- [ ] Yes, within minutes (5 points)
- [ ] Usually, within an hour (3 points)
- [ ] Sometimes, takes hours (1 point)
- [ ] No, constant uncertainty (0 points)

B5. Are critical alerts automatically prioritized and escalated?

- [ ] Yes, automated escalation (5 points)
- [ ] Manual escalation process (2 points)
- [ ] No prioritization system (0 points)

Section B Score: _____ / 25

Section C: Detection Capabilities (Maximum 25 points)

C1. Do you monitor all endpoints (workstations, servers, mobile devices)?

- [ ] Yes, 100% coverage (5 points)
- [ ] Most endpoints (>75%) (3 points)
- [ ] Some endpoints (<75%) (1 point)
- [ ] No endpoint monitoring (0 points)

C2. Is your network traffic analyzed for threats?

- [ ] Yes, comprehensive analysis (5 points)
- [ ] Basic traffic monitoring (2 points)
- [ ] No network analysis (0 points)

C3. Are your cloud environments and applications monitored?

- [ ] Yes, all cloud resources (5 points)
- [ ] Partial cloud monitoring (2 points)
- [ ] No cloud monitoring (0 points)

C4. Do you use behavioral analytics to detect anomalies?

- [ ] Yes, advanced analytics (5 points)
- [ ] Basic anomaly detection (2 points)
- [ ] No behavioral analysis (0 points)

C5. Is threat intelligence integrated into your security monitoring?

- [ ] Yes, real-time threat feeds (5 points)
- [ ] Basic threat intelligence (2 points)

- [ ] No threat intelligence (0 points)

Section C Score: _____ / 25

Section D: Response Readiness (Maximum 25 points)

D1. Do you have a documented incident response plan?

- [ ] Yes, comprehensive and current (5 points)
- [ ] Yes, but needs updating (2 points)
- [ ] No formal plan (0 points)

D2. How often do you test your incident response procedures?

- [ ] Quarterly or more (5 points)
- [ ] Annually (3 points)
- [ ] Rarely (1 point)
- [ ] Never tested (0 points)

D3. Can you contain identified threats within 30 minutes?

- [ ] Yes, automated containment (5 points)
- [ ] Within 1 hour (3 points)
- [ ] Within 1 day (1 point)
- [ ] Longer or unknown (0 points)

D4. Do you have forensic investigation capabilities?

- [ ] Yes, comprehensive forensics (5 points)
- [ ] Limited capabilities (2 points)
- [ ] No forensic capabilities (0 points)

D5. How often are backup and recovery procedures tested?

- [ ] Monthly (5 points)
- [ ] Quarterly (3 points)

- [ ] Annually (1 point)
- [ ] Never tested (0 points)

Section D Score: _____ / 25

Calculate Your Total Score

Section	Your Score	Maximum
A: Coverage Hours	_____	25
B: Alert Management	_____	25
C: Detection Capabilities	_____	25
D: Response Readiness	_____	25
TOTAL	_____	**100**

Your Risk Level

✅ 80-100 Points: Low Risk

Congratulations! You have strong security monitoring coverage.

Your Strengths:

- Comprehensive monitoring coverage
- Effective alert management
- Strong detection capabilities
- Prepared for incident response

Recommendations:

- Continue regular testing and optimization
- Consider advanced threat hunting capabilities
- Evaluate emerging threat detection technologies
- Share best practices with industry peers

⚠️ 50-79 Points: Moderate Risk

Caution: Significant gaps exist in your monitoring that attackers can exploit.

Key Vulnerabilities:

- Incomplete after-hours coverage
- Alert overload or missed alerts
- Limited detection capabilities
- Response procedures need improvement

Immediate Recommendations:

- Prioritize 24/7 coverage for critical systems
- Implement automated alert triage
- Consider managed SOC services to fill gaps
- Develop and test incident response procedures

🔴 25-49 Points: High Risk

Warning: Your business is vulnerable to undetected attacks.

Critical Gaps:

- Major coverage blind spots (nights/weekends)
- Overwhelming alert volume with low investigation rate
- Limited threat detection capabilities
- Unprepared for incident response

Urgent Actions Required:

- Implement basic 24/7 alerting immediately
- Strong candidate for SOC-as-a-Service
- Develop incident response plan
- Conduct security awareness training

🚨 0-24 Points: Critical Risk

URGENT: You're operating without essential security monitoring.

Extreme Vulnerabilities:

- No meaningful security monitoring
- Attacks likely going undetected

- No incident response capability
- 60% of SMBs fail within 6 months of a major breach

Emergency Response Needed:

- Immediate professional security assessment
- Deploy basic security monitoring tools
- Urgent need for professional security operations
- Consider emergency incident response retainer

Key Risk Metrics Based on Your Score

Coverage Gap Analysis

Risk Level	Hours/Week Without Monitoring	Time to Detect Threats	Annual Risk Exposure
Low Risk	0-20 hours	< 24 hours	< $100,000
Moderate Risk	20-80 hours	1-7 days	$100,000 - $500,000
High Risk	80-120 hours	7-30 days	$500,000 - $2,000,000
Critical Risk	120-168 hours	30+ days (Industry avg: 277)	> $2,000,000

Remember: The industry average time to detect a breach is 277 days for organizations without proper monitoring!

Recommended Next Steps

Immediate Actions (This Week)

1. **Enable basic alerting** on all critical systems
2. **Document** current security tools and coverage
3. **Test** your backup recovery process
4. **Review** cyber insurance coverage
5. **Establish** emergency contact list

30-Day Improvements

1. **Evaluate SOC-as-a-Service options** for 24/7 coverage
2. **Implement SIEM** if not currently in place
3. **Conduct tabletop exercise** for incident response
4. **Review and update** security policies
5. **Train staff** on security awareness

90-Day Strategic Goals

1. **Achieve 24/7 monitoring** capability
2. **Implement automated threat detection**
3. **Establish incident response plan** and test it
4. **Deploy endpoint detection** on all systems
5. **Integrate threat intelligence** feeds

Understanding SOC-as-a-Service ROI

Cost Comparison

Solution	Annual Cost	Coverage	Detection Time
In-House SOC	$2.7M+	If fully staffed	Varies
Traditional MSSP	$60K-180K	Monitoring only	30-60 minutes
No SOC	$4.88M (breach cost)	None	277 days
SOCaaS	**$96K-360K**	**24/7/365**	**3 minutes**

SOCaaS Benefits

- ✓ 70-80% cost savings vs. in-house SOC
- ✓ 24/7/365 expert monitoring and response
- ✓ 3-minute average threat detection
- ✓ 40% reduction in false positives
- ✓ Included incident response
- ✓ Compliance reporting

Don't Wait for the Weekend Attack

Every weekend without monitoring is a gamble with your business's survival.

75% of attacks occur outside business hours

67% of SMBs have no after-hours monitoring

60% of SMBs fail within 6 months of a major breach

$150,000 average cost when ransomware succeeds

Ready to Close Your Security Monitoring Gaps?

Schedule a free consultation to discuss your assessment results and explore how InventiveHQ's SOC-as-a-Service can protect your business:

✓ **24/7/365 expert monitoring** - Never leave your business exposed

✓ **3-minute threat detection** - Stop attacks before they spread

✓ **95% accurate threat classification** - Focus on real threats, not false alarms

✓ **Complete incident response** - From detection to recovery

Contact InventiveHQ

Don't let another weekend pass unprotected.

📧 **Email:** info@inventivehq.com

📞 **Phone:** (866) 903-2097

🌐 **Web:** inventivehq.com/security-operations-center-soc/
