Intelligent iT

24/7 SOC vs. Business Hours Security

Threats Don't Respect Your Schedule

Cyber threats operate around the clock. Organizations relying on business-hours-only security create predictable windows where attacks can propagate unchecked. This condensed analysis examines the case for 24/7 monitoring.

The Coverage Gap Problem

Business-hours-only monitoring covers just 40 hours per week—leaving 128 unmonitored hours where attacks can proliferate. Fastest intrusions reach data exfiltration in 72 minutes. An after-hours attack on Friday evening could go undetected until Monday morning, providing attackers with an entire weekend to establish persistence, exfiltrate data, or deploy ransomware.

Adversaries know which organizations have gaps and deliberately target them.

Financial Reality

24/7 SOC operations cost 60-80% more than business-hours coverage. Average SMB breaches cost $140K-$254K. A single undetected breach justifies multiple years of 24/7

operations. For organizations with sensitive data or compliance requirements, 24/7 monitoring is non-negotiable.

Implementation Reality

True 24/7 monitoring requires three components: intelligent detection systems that distinguish signal from noise, qualified analysts available at all hours, and rapid response procedures. Many organizations mistake having alerts flowing to ticketing systems as "24/7 monitoring"—the difference between alerts and actual response is everything.

Key Statistics

72 minutes: Time for fastest intrusions to reach data exfiltration | 44%: Breaches now involve ransomware | 60%: Attacked SMBs that close within 6 months

The Path Forward

The question isn't whether to implement 24/7 monitoring—it's how to do so efficiently. Solutions that automate detection and response can reduce staffing burden while maintaining protection quality. Intelligent iT's Unified Core platform enables true 24/7 capability through AI-enhanced threat detection and automated response, helping organizations achieve protection without proportional staffing increases.

In today's threat landscape, after-hours coverage gaps are simply unacceptable. The cost of protection is far lower than the cost of undetected breaches.