Blumira

The SIEM Checklist for MSPs

Make a confident security operations platform decision.

Selecting a security operations platform isn't just about your own tech stack. It's about the foundation of the services you provide to your clients. This decision impacts your team's efficiency, your service margins, and the trust your clients place in you. Use this checklist to evaluate how a partner will help you scale your security offering without needing to hire an army of analysts.

How to Use This Checklist

To make a confident choice for your MSP, we recommend this three-step approach:

1. **Assess Your Operations:** Identify the manual tasks currently slowing your team down and where you have visibility gaps across your client base.
2. **Compare Vendors:** Use these criteria to see if a vendor is just selling you a tool or if they are actually built to support the MSP business model.
3. **Bridge the Gap:** Review the "How Blumira Helps" callouts to see how we help you deliver enterprise-grade security that works on day one.

Questions Every MSP Should Ask a Security Vendor

- Does your pricing scale with my client's growth?
- How long does deployment typically take?
- What happens if we exceed our data limits?
- Can we see a demo with our actual use cases?
- What does your support response time look like?

Define Your Security Priorities

Aligning your security operations with your business goals allows you to offer more value without increasing your overhead. Check out the CSF Quick Start Guide as a start.

- **Identify Top Threats:** Define your clients' top security risks, such as data breaches, ransomware, or insider threats.
- **Prioritize Critical Assets:** Determine which systems require the most protection, such as cloud environments or intellectual property.
- **Define Primary Focus:** Are you looking to provide 24/7 threat detection, satisfy cyber insurance requirements, or offer a fully managed incident response service?
- **Assess Maturity:** Are you in "reactive mode" (fixing things when they break) or moving to "proactive leadership" (preventing threats before they impact the client)?

Blumira identifies real attack patterns *across cloud, network, and endpoints, not just noise. You can scope threats like ransomware in a single console and deliver automated executive summaries that prove risk mitigation to your clients.*

Ensure Compliance & Regulatory Alignment

For most of your clients, security is driven by the need to stay compliant or insurable. Your SIEM should make this an easy "win" for your team.

- **Map Client Regulations:** Meet all relevant compliance mandates (e.g., HIPAA, GDPR, PCI DSS, NIST).
- **Define Data Retention:** Determine how long logs must be stored (90 days, 1 year, or multiple years).
- **Identify Reporting Needs:** List required outputs, such as pre-built compliance reports or audit trail documentation.

Blumira built compliance and cyber insurance *requirements into the platform with 24/7 automated monitoring, 365-day retention, and ready-made reports for 13+ frameworks including HIPAA, SOC 2, and NIST.*

Map Your Technical Environment

Your SIEM must play well with the tools you already use, or it becomes just another silo for your team to manage.

- **Audit Client Architectures:** Most MSPs manage a mix. Confirm your solution can handle cloud-only, hybrid, and multi-cloud environments without requiring different workflows for each.
- **Catalog Data Sources:** List all systems to be monitored, including servers, network devices, and applications.
- **Plan Security Integrations:** Identify current tools that must integrate with the SIEM, such as EDR/XDR or firewalls.

Blumira has 75+ pre-built integrations *that easily help you monitor Windows, Mac, cloud environments, network devices, and identity platforms from one unified console. No complex configurations or professional services required. Get complete visibility across hybrid and multi-cloud environments.*

Assess Your Operational Capacity

You don't have unlimited hands. The right partner should feel like an extension of your team, not a burden on it.

- **Evaluate Internal Talent:** Does your team have dedicated security analysts, or do your general technicians handle alerts? Look for a platform that provides "automated expertise."
- **Set Detection Requirements:** Do you want to write your own detection rules (complex) or have them managed for you (efficient)?
- **Select a Support Model:** Ensure you have access to security experts who understand the "multi-tenant" reality of an MSP.

Blumira's *"SOC Auto-Focus" applies eight years of security expertise documented by our team to every alert, providing guided playbooks so your general technicians can respond like seasoned security pros. If a critical threat is detected, you can instantly isolate compromised devices with one click to prevent a client-wide disaster.*

Plan Your Budget & Protect Your Margins

For most MSPs, unpredictable costs are the enemy of profitability. Your security platform should be a predictable line item.

- **Confirm the Support Model:** Define your needs for 24/7 support versus business-hour support.
- **Confirm the Pricing Model:** Avoid "per-GB" or "ingestion-based" pricing. These models penalize you when your clients grow or when a security event generates a spike in logs, exactly when you need the tool most.
- **Calculate Total Cost of Ownership:** Include licensing, professional services, training, ongoing support, and potential overage fees.
- **Identify Hidden Costs:** Ask about implementation fees, data overage penalties, and upgrade costs.

With Blumira, *there are no more "oops, we went over" moments with your finance team. You get predictable, transparent pricing based on protected users, not data volume. With unlimited log ingestion and year-long retention included, you can scale your MSP with confidence, knowing your margins are protected.*

Ready to see How Blumira Stacks Up?

We understand that as an MSP, you aren't just buying a tool—you're choosing a partner to help you grow. Our team is here to help you navigate these considerations and show you how to turn security into a profit center.

Speak With Our Team