Top 6 Common Security Mistakes

[AND HOW TO AVOID THEM]

We have signed you up for Blumira's **Free SIEM** edition. With it, you get access to everything below for free:

- Up to 3 cloud integrations, including Microsoft 365, for log collection & threat analysis*
- 14 days of log retention
- Managed detections, detection rule insight
- Response playbooks with instructions on remediation
- Dashboard summary & basic reporting
- Notifications (voice, email & text) of findings

**Choose from Microsoft 365, Gsuite, Duo Security, SentinelOne, Cisco Umbrella, Webroot and/or Mimecast*

This is a great first step toward securing your company.

But that's just scratching the surface. The Free SIEM doesn't check all of the boxes like **SIEM Pro, SIEM+ and XDR** Editions do. Without certain capabilities, you could be subject to compliance fines, driving up your cyber insurance premiums, or putting your company officers at risk of being held liable in the case of a breach — without even realizing it.

Blumira's paid editions allow you to meet compliance, support remote work, automate threat response for faster time to security and much more.

These are some key security mistakes business owners make, the consequences, and how Blumira helps you solve them.

Mistake #1: You're not retaining data for at least 90 days or 1 year.
Result: You're in violation of CIS, NIST, PCI DSS and other compliance regulations that require 1 year of audit log history. You also have no way to look back at past events for forensic investigations or incident response, so it's harder to trace the events of an attack to figure out what happened and how to prevent it in the future.

Solution: Make sure you're keeping your logs long enough to satisfy compliance and have a tamper-free backup of your data by upgrading to Blumira's SIEM+ or XDR Platform for one year of log retention.

Mistake #2: You're not capturing endpoint logs and applying advanced detections to them.
Result: Without insight into remote workers, you're left with a critical security gap. Cyber insurance may ask for endpoint detection & response. Without that box checked, your cyber insurance premiums may skyrocket.

Solution: Get advanced endpoint visibility and response with **Blumira Agent**, available in Blumira's SIEM+ or XDR Platform editions. The agent applies detection rules to identify attacker behavior that other EDR/AV tools may miss, then allows you to isolate affected endpoints immediately.

Blumira

Mistake #3: You don't have 24/7 security support.
Result: Cyber insurance may ask if you have a SOC or SIEM. But you may also run into issues when you need security advice, assistance with incident response, or have questions about onboarding – not easy to troubleshoot without hiring expensive security staff.

Solution: Upgrade to Blumira's SIEM Pro, SIEM+ or XDR Platform for access to Blumira's dedicated Solution Architects for successful onboarding guidance, or for emergency after hours Security Operations (SecOps) support for critical priority issues.

Mistake #4: You're manually responding to every ticket.
Result: Aside from reducing business productivity by draining your time, this can mean there's a critical gap between when a threat is initially detected and when your team is able to respond to it – a period of time that could result in a ransomware infection or a breach.

Solution: Gain automated response with Blumira's **XDR Platform** – the ability to immediately contain an affected endpoint or block traffic from known malicious sources, a way to extend the abilities of your small team and close the attacker gap.

Mistake #5: You only have a few cloud apps sending logs to a SIEM.
Result: Without coverage for all system logs, you have less overall visibility into your entire environment. It's also harder to gather relevant information when a serious security threat occurs. Attackers will delete or alter logs to cover their tracks, leaving you without any evidence in the case of a breach – which is why some compliance frameworks mandate that you must have a way to ensure logs stay intact.

Solution: Avoid violating compliance and gain greater visibility by unlocking access to more than 70 cloud and on-prem integrations with SIEM Pro, SIEM+ and XDR Platform.

Mistake #6: Your team is wasting time chasing after false positives.
Result: Cutting down on the number of alerts you get is key to saving time spent tracking down, triaging and investigating false positives that send your team down rabbit holes – meaning less time prioritizing initiatives and paying attention to actually-critical alerts.

Solution: Customize your detection rules by filtering out known safe activity by user, IP address, and more with Blumira's Detection Filters, available with SIEM Pro, SIEM+ and XDR Platform.

> I don't have the staff dedicated to sit and read logs all day or with the skillset to analyze our data. **We chose Blumira for its simplicity** – I needed a solution that would simplify, consolidate and show me what I really need to see.

Jim Paolicelli, IT Director
Atlantic Constructors