

## Blumira's 24/7 SecOps Team

With our SIEM + XDR platform and expert teams combined, **you get 24/7 coverage** -- there's no need to hire full-time analysts to manage your security.

### Blumira's platform & teams do the work for you:



- **Daily log review & log monitoring** -- Easily meet compliance with automated review of your logs for suspicious activity
- **Log parsing & data standardization** -- Other SIEMs require developers to parse your data; Blumira's engineers build it into the platform
- **Threat hunting, writing, testing & tuning rules** -- Other SIEMs require experts to develop detections; Blumira's security engineers do it at scale for the platform while tuning detections to reduce noisy alerts
- **Experienced security team available 24/7** -- On standby to help you with critical priority issues and assist with incidents & investigation

*Blumira's customer experience is the **bridge for our customers between the IT team that they have, which could be quite small, and our detection engineers, who provide the security expertise that they don't have in-house.** – Heidi Craun, Blumira VP of CX*

*The faster the response, the better the security outcome.*

# 20 MINUTES

**BLUMIRA'S AVERAGE  
RESPONSE TIME**

**VS.**

**HOURS, DAYS & WEEKS  
MDR RESPONSE TIME**

*Every minute counts in a security incident situation.*

### OTHER SOLUTIONS

- At least 1-2 full-time employees are required to set up & run other solutions
- Managed detection & response (MDR) analysts are often inexperienced & stretched thin between 50-75 customers
- Customers report threat response delays of hours to days & weeks with MDRs
- MDRs still require your team to remediate incidents, since they lack the local context you have about your users & organization
- There's no one solution that can fully handle detection & response without your team

*The Solutions Architect gave me recommendations, checked my environment with a scan and set up a report I was looking for. **I feel like I have another employee watching security for us. This is great for a small organization.** – Les Neely, System Admin, Upward Sports*

## 24/7 SecOps: An Extension of Your Team

### INCIDENT DETECTION ENGINEERS



The incident detection team writes detection rules that power Blumira's platform to identify indicators of compromise early & often for our customers:

- Threat hunting & releasing new detections every 2 weeks
- Findings are sent within minutes of initial detection for the fastest response times
- Proactive outreach to customers about malicious activity seen in their environment

*Compared to other vendors, the ability to get someone that knows what they're talking about is invaluable. We work really well with Blumira's engineering team and value the accessibility to Blumira's support staff and the brains behind the platform. -- Steve Gatton, VP of IT, Fechheimer*

### TECHNICAL SUPPORT



Our Technical Support Analysts troubleshoot any issues you may have with the platform, in addition to:

- Listening to you and bringing your insights directly to Product/Engineering teams
- Advocating for Blumira feature additions & usability enhancements



**100% CSAT SCORE**  
CUSTOMER SATISFACTION SCORE  
RATING BLUMIRA'S TECH/SECURITY TEAMS

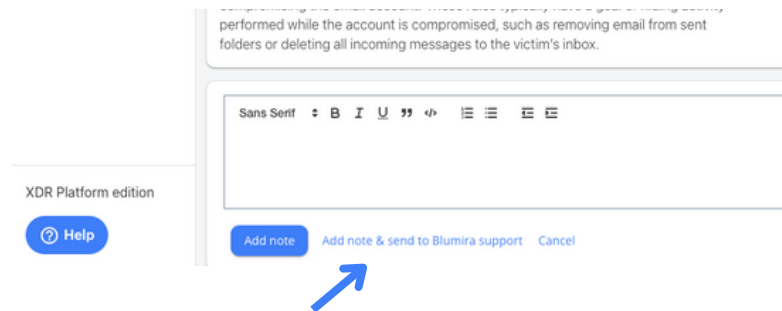
*Your entire support team has been awesome. They are willing to go out of their way for you. Every time I open a ticket or have any other type of interaction – the experience has been great. **Blumira is at the top of the list when it comes to customer support.***  
-- Frank DeLuca, President, The CTO Agency

### SOLUTION ARCHITECTS



Our Solution Architects (SAs) help customers proactively to ensure long-term success & increase their confidence in their own security:

- Guided onboarding for their environment
- Recommendations on how to collect logs
- Advice on general security posture



**Direct message 24/7 SecOps, in-app for help**

### SECURITY OPERATIONS



Our experienced & responsive SecOps team is a dedicated group of security experts:

- On standby to help you tailor Blumira security detections for your specific needs
- Help you understand Blumira's security findings
- Supports you 24/7 for critical security issues

### DEMO XDR TODAY

Blumira makes security easy and effective for SMBs, helping them detect and respond to cybersecurity threats faster to stop breaches and ransomware.

Contact us to see a demo of Blumira's SIEM + XDR platform.

Visit [blumira.com](https://blumira.com)