

Blumira vs. MDRs

Managed detection & response (MDR) vendors may sound too good to be true – they come with promises of dedicated SOC experts to handle all of your threat detection and remediation. But the reality is, MDRs can result in delayed response times and poor security outcomes.

With Blumira's SIEM + XDR platform and expert teams combined, you get 24/7 coverage at lower total cost of ownership and no need to hire full-time security experts.

“Being a small company, we were looking at what we get for the value – **Blumira was coming in at less than half the price of what Arctic Wolf wanted.** I couldn't justify where that extra value was coming from, with Arctic Wolf. -- IT Manager, Small Automotive Company

MDR CHALLENGES



- Threat response is not actually hands-off, still requiring your IT team
- Major delays in response (hours to weeks) puts you at high risk
- Inexperienced SOC analysts are handling your security

BLUMIRA SOLUTION



- Alerts are sent directly to you in under a minute of initial detection
- Alerts include analysis, easy steps to take for faster remediation
- Experienced SOC team available 24/7 to help you with critical priority issues – an average response time of 20 min

RESPONSE REALITY



When talking to Arctic Wolf, the sales team pitched them the offer to do all of their remediation for them.

Well, you [Arctic Wolf] don't know my environment – so I'm not ok with that.

What I want is a solution that generates alerts for me, with a company that would be able to help me if I need to investigate further. That's where Blumira came in.

SECURITY VALUE



Pricing played a role the small company considered how to get the best return out of their security investments.

*The price was also a huge factor. To me, it was a great starting point; that's how I sold it to the owners – here's what we could get. **Arctic Wolf is one of the leading providers in the market, but it cost \$20,000 more.***

I'd rather put Blumira in place, knowing that it's going to cover all of our needs, and then use that extra money to address our other security concerns.

The Truth About MDRs

TIME-CONSUMING FOR YOUR TEAM

- They claim to “handle all of your security for you” – but without local context, they cannot actually remediate or close out a ticket without involving your IT team to verify a legitimate threat or not
- That means your team will still be pulled into threat response and remediation regularly

INEXPERIENCED ANALYSTS

- Many MDRs put Level 1 SOC analysts with no experience into the position of handling your security on a regular basis
- This high-stress role results in a great deal of churn as entry-level analysts move up in their career, leaving you with a revolving door of third-party support

MAJOR DELAYS IN THREAT RESPONSE

- Some MDRs (like Arctic Wolf) have their SOC analysts supporting upwards of 50-75 customers at one time
- With that many customers to attend to, their analysts are stretched very thin – which results in major reported delays in threat response from hours to days to a week

*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

BLUMIRA 24/7 SECOPS



Blumira’s experienced & responsive SecOps team is a dedicated group of security experts:

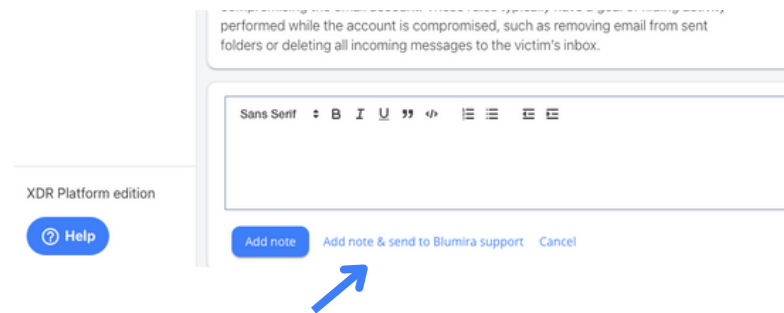
- On standby to help you tailor Blumira security detections for your specific needs
- Help you understand Blumira’s security findings
- Supports you 24/7 for critical security issues

Blumira’s security, architect, incident detection engineers and tech support teams provide onboarding, proactive threat hunting, detection rule management and more -- all at no additional cost.

20 MIN.

BLUMIRA AVG. RESPONSE TIME

COMPARED TO MDRS’ HOURS/DAYS/WKS



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



100% CSAT SCORE

CUSTOMER SATISFACTION SCORE
RATING BLUMIRA’S TECH/SECURITY TEAMS

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