Blumira speeds time to market by building with LimaCharlie

Cloud SIEM provider Blumira is on a mission to deliver enterprise-grade security for SMBs. Last year, the company set out to build a remote end-point monitoring solution for small teams: Blumira Agent. The vision for Agent: a solution that could collect Windows endpoint logs and sendthem to Blumira's cloud SIEM platform for analysis, detection and threat response—without requiring additional infrastructure or management on the part of the customer. By leveraging LimaCharlie's SecOps Cloud Platform, Blumira was able to launch their ambitious new cybersecurity offering in just months.

Mature capabilities, delivered on demand

Blumira had the technical ability to build an end-to-end solution—but to accelerate their product launch, leadership decided against developing an endpoint agent on their own. The company began the search for a technology that would support Blumira Agent while integrating well with the rest of their cloud SIEM platform.

"The biggest challenge was finding a mature enough solution that we could build on quickly and still end up with something as good as what we had elsewhere," says Jake Payton, Director of Engineering at Blumira. "We also wanted a real partner during the development process."

After considering NXlog, winlogbeat, Telegraf, and a number of potential agents, Blumira found that LimaCharlie's SecOps Cloud Platform offered the best balance of capabilities, cost, and support.

LimaCharlie takes an unusual approach to cybersecurity. The company offers users an ecosystem of 100+ mature capabilities and integrations as cloud-native primitives. Similar to the way AWS provides IT capabilities and web services, LimaCharlie is a SecOps Cloud Platform in which everything is delivered on-demand, as-needed, and API-first—no contracts, price modeling, or fixed minimums required.

"LimaCharlie is like a box of Lego blocks for cybersecurity," says company co-founder Christopher Luft. "There is no one-size-fits-all solution to cybersecurity problems. Our approach gives teams the flexibility to build truly custom solutions."

COMPANY PROFILE

Blumira

FOUNDED
2018

HEADQUARTERS
Ann Arbor, Michigan

SECTOR
Financial services, government, critical infrastructure, public utilities, commercial, construction, retail, and healthcare.

COMPANY
Blumira's SIEM+XDR platform helps small and medium-sized businesses prevent breaches and ransomware by simplifying threat detection and response.

OBJECTIVE

Build a comprehensive endpoint monitoring solution for SMBs: a product capable of collecting Windows endpoint logs and sending them to the Blumira cloud SIEM platform for analysis, detection and threat response.

CHALLENGES

- Collect endpoint telemetry without requiring additional infrastructure or technical resources on the part of end users
- Source robust third-party technology in order to speed time to market
- Find a supportive technology partner to work with during development

Concept to GA in five months

As development began, Blumira noticed the advantages of working with an infrastructure-first, engineering-centric vendor.

One of LimaCharlie's core capabilities is multi-source telemetry ingestion. On end-points, this is accomplished via the lightweight, multi-platform LimaCharlie agent.

Telemetry data is pulled into the LimaCharlie cloud and standardized to a common data format. From there, data can be exported to any destination. This functionality gave Blumira excellent visibility into remote Windows endpoints without straining user resources—grabbing Windows events and log data from hosts and sending them to the Blumira cloud for processing. In addition, because the LimaCharlie agent is able to take action on endpoints, Blumira would also be able to monitor and/or halt ingestion and take response actions as needed.

Access to cloud-native primitives meant that Blumira's developers could integrate advanced capabilities into their existing SIEM infrastructure quickly and easily. This was often as simple as setting up an API call between the two platforms, and was essential in shortening time to market. Development work began in August 2022, and Blumira Agent launched in January 2023. In the time that most vendors would take to perform feasibility studies, Blumira had delivered an advanced remote endpoint monitoring solution for SMBs.

Blumira says that the product has been a resounding success. Agent is the powerful and easy-to-use solution that the company had envisioned. Users find the installation process to be fast and simple. After installation, management is hands-off, as intended.

As for the experience of building with LimaCharlie, Blumira was extremely satisfied: "At every step of the way, the technology more than met our needs," says Payton. "And it was always easy to get information and guidance. If we had a question, we got the answers we needed very, very quickly. The LimaCharlie team was a joy to work with."

A platform built for builders

For Blumira, an added benefit of working with LimaCharlie was that they didn't have to purchase features or capabilities that they weren't going to use. Built on an advanced Detection, Automation, and Response Engine, the LimaCharlie SecOps Cloud Platform is extensive, and can also be used for MSSPs, DFIR, and enterprise SOCs.

However, because of LimaCharlie's unique delivery model, Blumira's developers were able to choose only the capabilities that worked for them and leave the rest aside for the future—a future Payton views with optimism:

"We aren't even close to using all of the capabilities in LimaCharlie. I'm already excited about this partnership—and about where it's going to go in the years to come."

In terms of their own vision for the future, LimaCharlie believes that the on-demand, engineering-centric model they've pioneered is the way to move the industry forward.

"LimaCharlie is security done differently—and our technology partners benefit from that difference," says Luft. "It's a very new approach, but we feel that in time cyber-security professionals will stop asking "Should we do it this way" and will instead ask "Why would we do it any other way?"

SOLUTION

- Build on LimaCharlie's multi-platform agent
- Work with LimaCharlie developers to integrate the new product into the Blumira cloud SIEM platform

BENEFITS

- Greatly shortened time to market
- A product that met or exceeded expectations and left end users satisfied
- On-demand access to mature security capabilities—no contracts or paying for unwanted features
- A genuine technology partnership with strong long-term potential

I would highly recommend LimaCharlie to anyone wanting to access advanced cybersecurity capabilities, extend what they're currently doing, or even build something from scratch. The platform is robust, performant, safe, and very powerful. Go for it!

Jake Peyton
Director of Engineering, Blumira

ABOUT LIMACHARLIE

LimaCharlie is creating a new paradigm for security operations teams through the SecOps Cloud Platform. To learn more, book a demo, or try the SCP for free, visit **limacharlie.io**