

MDR firm saves \$100K per year with LimaCharlie SecOps Cloud Platform

Background

Recon Infosec is a managed detection and response (MDR) firm that offers enterprise-tier security services to small- and medium-sized organizations. With an unusual number of cybersecurity subject-matter experts on staff, Recon had been able to engineer a custom security stack using AWS, Elastic Compute Cloud, Elasticsearch, and various open-source tools. But as the MDR firm grew, it became clear that this DIY approach to infrastructure and tooling would not scale. There were increasing costs and complexity to maintaining a homegrown security stack. And the firm's orchestration, automation, and DevOps teams were spending too much time maintaining infrastructure instead of focusing on security operations.

Recon Infosec needed a simpler, more cost-effective solution—one that would match the savings they'd achieved with a custom stack *and* help them maintain best-in-class security operations. The firm found what it needed in the LimaCharlie SecOps Cloud Platform (SCP).

SecOps Cloud Platform delivers \$100K in savings

The SecOps Cloud Platform is a new paradigm for security operations. It is a unified cloud platform that does for cybersecurity what the IT public cloud did for IT. The SCP gives security teams the core capabilities and infrastructure they need: on-demand, pay-per-use, and API-first.

This approach offers multiple opportunities for cost savings:

- ◆ Unify tools and infrastructure in a single platform, reducing tool sprawl and eliminating one-off vendors.
- ◆ Input data from any source and output it to any destination to reduce spending on expensive SIEM solutions. Send only necessary data to higher-cost platforms while retaining the rest in a low-cost storage solution. All telemetry data is automatically retained for free for one year in the SCP in a normalized and searchable format, helping teams lower storage costs without losing access to rich data.
- ◆ All cybersecurity capabilities in the SCP are delivered via an on-demand, pay-per-use pricing model. Teams only pay for what they need—and can scale up or down as required.

COMPANY PROFILE



FOUNDED
2015

HEADQUARTERS
Austin, TX

SERVICES
MDR, SOC as a service, DFIR

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

COMPANY
Small- and medium-sized organizations seeking managed, enterprise-tier cybersecurity services.

98%

improvement in Mean Time to Respond (MTTR).

\$100K

in annual cost savings.

- ◆ Pure usage-based billing options are also available. This helps teams pre-deploy sensors in sleeper mode into client environments for just pennies per month.
- ◆ Pricing is fully transparent with no contracts, capacity planning, or price modeling—and no unexpected expenses. Pricing predictability enables smarter budgeting and better business decision-making.

After demoing the SCP, Recon Infosec decided to migrate its entire security stack to the platform. “I saw the potential immediately,” says Recon Infosec’s CTO and co-founder Eric Capuano. “We would be able to meet every capability we currently had—and instantaneously gain several we’d never had.” And even though Recon Infosec had already engineered an extraordinarily cost-effective security stack, switching to the SCP still resulted in substantial savings, reports Capuano: “On average, we’re looking at an annual cost savings of approximately \$100,000.”

Minutes to milliseconds. Ready to scale.

Recon Infosec also saw substantial technical and business operations benefits after the migration. The SCP endpoint agent provides robust, real-time EDR capabilities—allowing response actions to be taken on an endpoint within 100ms of an event. This, says Capuano, was a game-changer: “Our previous technology was at the cutting edge of open-source capabilities but our mean time to detect (MTTD) and mean time to respond (MTTR) were still measured in minutes. The SCP agent has improved our MTTD and MTTR by around 98%.”

In addition, the SCP’s inherent scalability has directly benefitted Recon Infosec’s business operations, setting the stage for future growth. “Our ability to onboard customers quickly and confidently has increased dramatically,” says Andrew Cook, Recon’s VP of Technology and Services, “because our ability to scale is no longer limited by our ability to maintain our security infrastructure.”

ABOUT LIMACHARLIE

LimaCharlie is a SecOps Cloud Platform that gives teams full control and visibility over their security posture—and solves problems of vendor lock-in, unpredictable pricing, and tool sprawl.

To see how LimaCharlie can help you reduce costs and simplify security operations, try our SecOps Cloud Platform for free or book a demo today at limacharlie.io

Note: This case study was produced in June 2023. Eric Capuano believed so strongly in the future of the SecOps Cloud Platform that he stepped into the role of Director at LimaCharlie in September 2023. He continues to serve as an advisor and board member at Recon Infosec.

CHALLENGES

- ◆ Reduce cost and complexity of homegrown security stack
- ◆ Maintain control over tooling, infrastructure, and security operations
- ◆ Meet or improve existing MDR capabilities

SOLUTION

- ◆ LimaCharlie SecOps Cloud Platform

BENEFITS

- ◆ Immediate cost savings of \$100K annually
- ◆ Team free to focus on security operations instead of infrastructure maintenance
- ◆ 98% improvement in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)



We would be able to meet every capability we currently had—and instantaneously gain several we’d never had.