MDR Firm Improves DFIR Capabilities with SecOps Cloud Platform

Background

Recon Infosec is a managed detection and response (MDR) provider for small- and medium-sized organizations. The firm's security engineering team had achieved remarkable success with a homegrown security stack. But as it expanded, Recon Infosec encountered increasing challenges in several areas of operation, including incident response (IR):

- Recon Infosec had developed sophisticated detection logics and workflows, but this complexity demanded intensive infrastructure maintenance and created a substantial burden for the firm's security engineering teams.
- Client IT environments were becoming more complex, requiring visibility well beyond the traditional endpoint. Cloud, containers, web apps, SaaS platforms, email, messaging, and more all had to be integrated into the MDR's service offering.
- Complex detections also resulted in a delay between an event firing and the alert making it to the SOC. Response times, even though measured in minutes, were still longer than desired.

However, after adopting the LimaCharlie SecOps Cloud Platform (SCP), Recon Infosec was able to solve many of its toughest challenges—including ones related to its digital forensic and incident response (DFIR) capabilities.

A unique approach to cybersecurity

The LimaCharlie SecOps Cloud Platform is a new paradigm for cybersecurity: a transformation comparable to what the IT public cloud did for IT. The SCP delivers the core components needed to secure and monitor any organization via a public cloud model: API-first, on-demand, and pay-per-use. For cybersecurity providers, this offers unprecedented ownership over their security stack and transparent, predictable pricing.

And as Recon Infosec discovered, many of the SCP's core capabilities directly benefit cybersecurity teams offering IR services:

Multi-tenancy lets teams manage multiple organizations from a single platform. In IR engagements, pre-configured tenants can be spun up in seconds—even for new clients.

Telemetry can be ingested from any source and run through the SCP's advanced Detection, Automation, and Response Engine. Teams gain complete visibility into a client's environment and wire-speed response capabilities.

Automation is integral to the SCP, allowing incident responders to define and execute automated response actions on endpoints in order to reduce response times and eliminate manual effort.

Usage-based billing allows MDRs and MSSPs to pre-deploy sensors to existing clients' environments and turn them on at a moment's notice for rapid response during an incident.

COMPANY PROFILE

RECON™ INFOSEC

FOUNDED
2015

HEADQUARTERS
Austin, TX

SERVICES
MDR, DFIR, SOC as a service

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

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

98%

improvement in Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)

“The SCP solved many things so well that we simply no longer had to worry about them,” says Andrew Cook, Chief Technology Officer at Recon InfoSec. “The platform also aligned with our engineering-centric approach to cybersecurity, which let us focus on our core value proposition: being at the cutting edge of security operations.”

Faster onboarding. Improved response times. Real-world results.

Recon Infosec soon saw the benefits of the SCP during real-world IR scenarios.

The SCP’s multi-tenant architecture helped the firm security teams deploy far more rapidly to client environments during IR engagements. In addition, the SCP’s lightweight, multi-platform agent directly improved Recon Infosec’s response capabilities.

“As an MDR, IR is one of our core offerings—and our goal is to finish the fight,” says Cook. “The SCP agent helps us do that by giving us access to client environments and letting us take fast action on endpoints during an incident: automating alerting, killing processes, isolating hosts, and more.”

The SCP agent, in combination with the platform’s robust automation capabilities, also helped speed Recon’s overall response times. After switching to the SCP, the firm’s mean time to detect (MTTD) and mean time to respond (MTTR) improved by approximately 98%, delivering tangible value to their customers.

“We had a big IR win early on with the SCP when we were detecting a behavior related to the SocGholish malware family,” recalls Cook. “The detection fired within a minute of getting into the SOC. We immediately quarantined the compromised machine, alerted the customer, and began a full response. Had that response been delayed by even 15 minutes, it could have evolved into something much worse.”

The future of cybersecurity

The SecOps Cloud Platform is designed to give security professionals full control over their infrastructure and tooling—enabling teams to do things that are simply not possible with any other vendor.

Cook says this approach has greatly benefited his company: “We wouldn't be as successful as we are now if we had to abdicate our effectiveness to another security provider; if we were only middlemen to a bigger vendor. There's just so much control within the SCP to develop your own vision for how security operations should work.”

Looking to the future, Recon Infosec says that the platform has opened up opportunities to scale—and to expand into new markets and pursue larger customers.

“We no longer have concerns about what it means to double our infrastructure, endpoint count, or even our customer base,” says Cook. “When we have a new deal, there's no longer any discussion around ‘can the stack handle it?’ From a scalability standpoint, we now feel completely unbounded—which is a huge relief!”

ABOUT LIMACHARLIE

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

CHALLENGES

- Solve key infrastructure challenges while retaining control over the security stack
- Gain greater visibility into client environments
- Improve incident response (IR) timelines
- Onboard customers more quickly during IR engagements

SOLUTION

- LimaCharlie SecOps Cloud Platform

BENEFITS

- Powerful, flexible platform for advanced security operations
- Team free to focus on security operations instead of infrastructure maintenance
- Better visibility into client environments and significantly improved response times
- Multi-tenant architecture makes onboarding new clients fast and easy

> “From a scalability standpoint, we now feel completely unbounded.