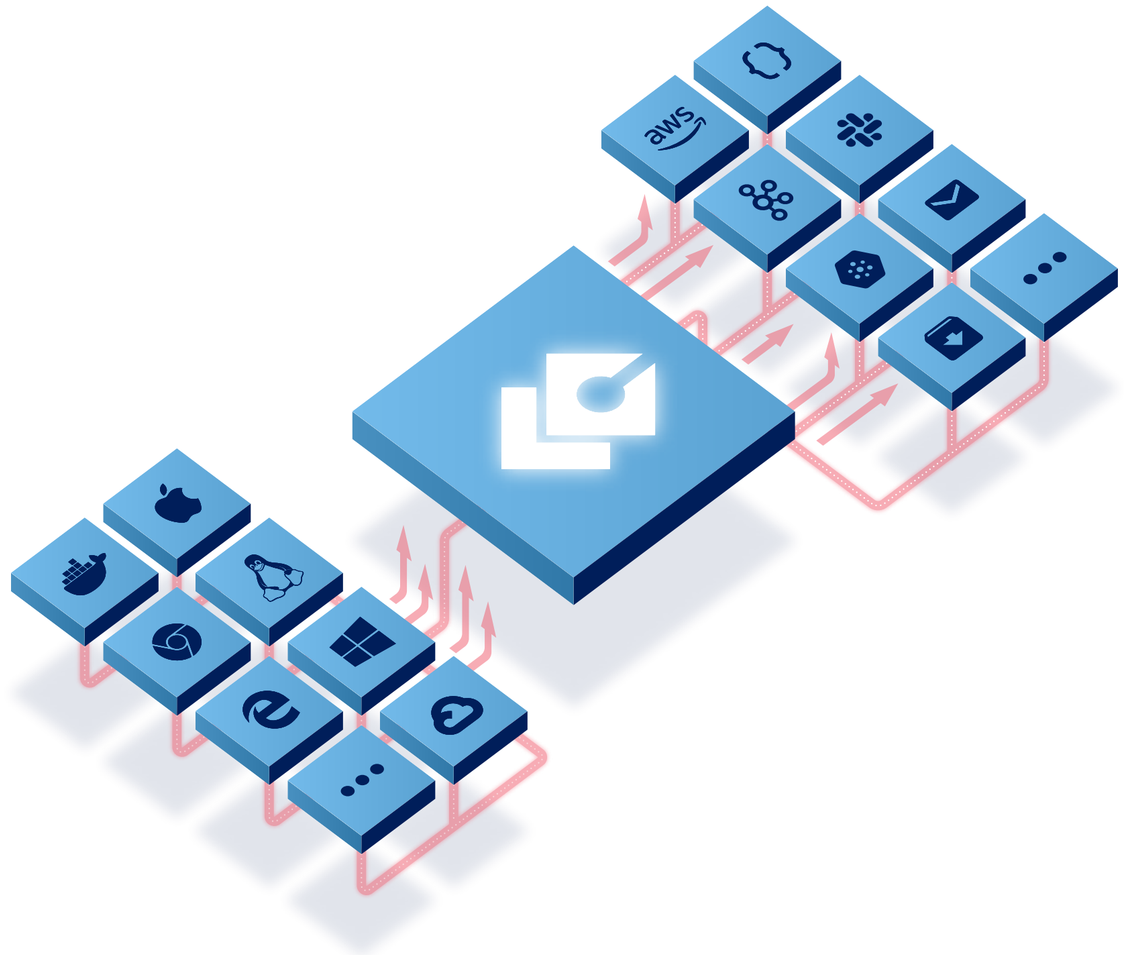
LimaCharlie

CASE STUDY

LimaCharlie Helps a DFIR Firm Respond to a Supply Chain Attack And Expand Their Business



EXECUTIVE SUMMARY

For privacy reasons, this case study has been anonymized. Referral contacts are available upon request.

A large retail company discovered that they had been affected by a supply chain attack, and called in a DFIR firm to help. Using LimaCharlie tools, the incident response team was able to investigate and contain the breach quickly and without having to take the retail company's POS systems offline. They then deployed a remediation package and took steps to harden the company's network against future attacks. Throughout the engagement, LimaCharlie's SaaS-like approach to cybersecurity was key to a fast and effective response. Long term, it also helped the DFIR company convert the customer into a permanent MDR account.

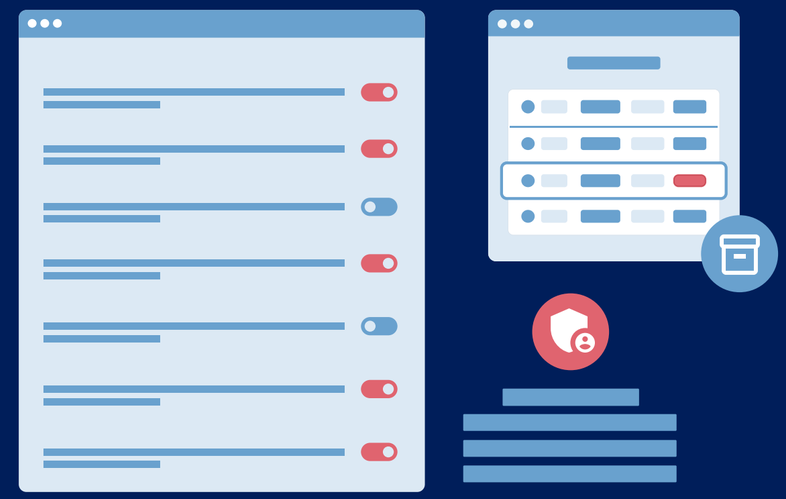
High-profile attack. High-stakes IR.

When the SolarWinds supply chain attack made headlines in December 2020, businesses everywhere were anxious to learn if they'd been affected.

At one large North American retailer, an internal IT team began a preliminary investigation based on IOCs published by Microsoft. They quickly realized that they had been breached, and called in a specialist DFIR company to help.

The incident response team found themselves facing a challenging situation. Because the SolarWinds attack had received so much media coverage, there was a significant risk that the bad actors would try to exfiltrate as much data as possible before their backdoors started shutting down all over the world.

In addition, the retailer was using a networked POS system to process millions of dollars in sales per day. The company lacked the internal tools required to lock down its own network and prevent data exfiltration. But taking the POS system offline to contain the breach — even briefly — would be extremely costly.



“So much easier”

Because the IR team was using LimaCharlie as its primary operational tool, they were well prepared for this type of engagement. LimaCharlie’s unique approach to cybersecurity was instrumental in helping the IR team hit the ground running.

The company provides a growing range of solutions for security teams, including EDR/XDR, SASE, and artifact ingestion. Unlike other vendors, LimaCharlie takes a SaaS-like approach to their tools and infrastructure. Everything is delivered on demand, via a self-service model. No fixed contracts are required, since all pricing is usage based. As LimaCharlie co-founder Christopher Luft puts it: “Think AWS, but for cybersecurity”.

During the IR engagement, this model provided a clear benefit in terms of operational efficiency. As one of the responders noted, “Since LimaCharlie is self-serve, we moved at our speed — no contracts or sales people in the way. We were running at scale within a few hours of beginning the engagement”. This is a sharp contrast to other offerings on the market, they added, saying that “it’s been so much easier working with LimaCharlie than any other vendor we’ve used before”.

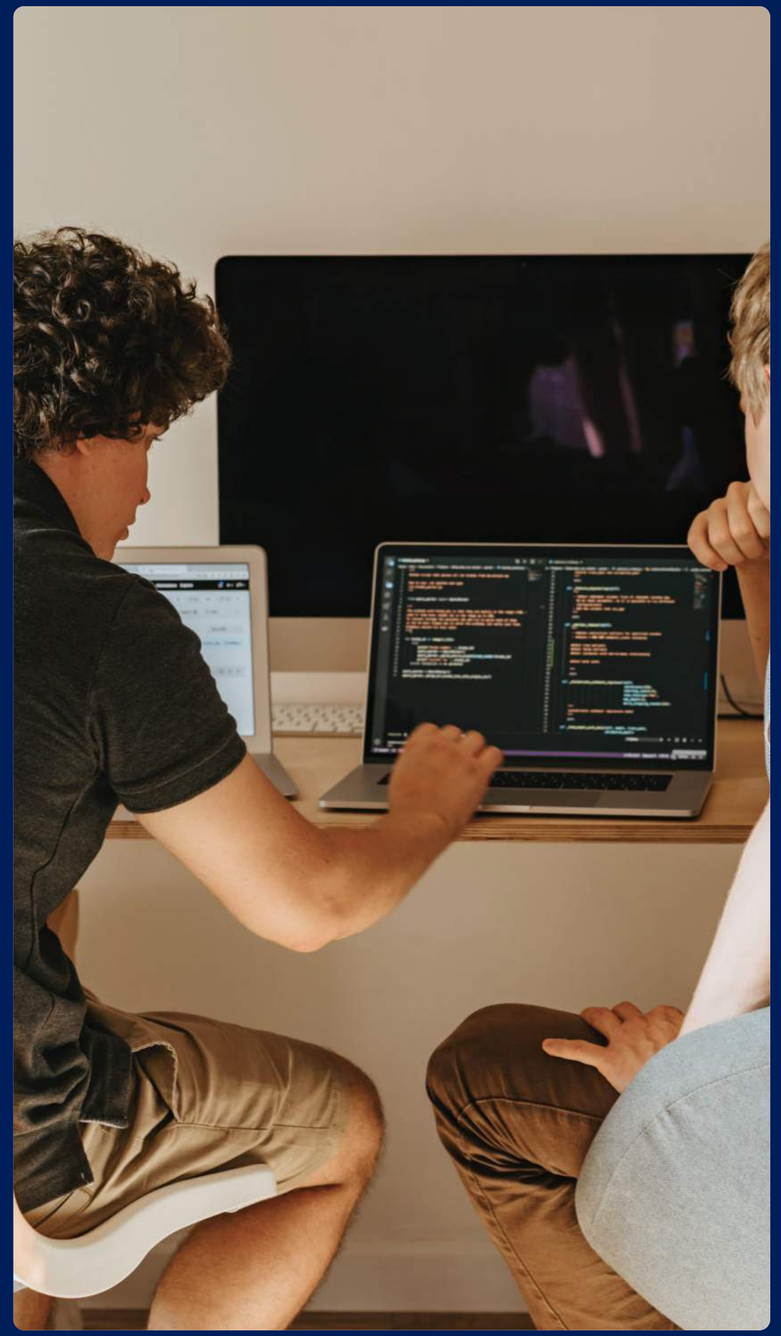
> Since LimaCharlie is self-serve, we moved at our speed — no contracts or sales people in the way.
>
> —Lead Security Operations

The responders began by installing the LimaCharlie agent on over 10,000 endpoints across the retailer's network. The process was straightforward, since LimaCharlie agents can be deployed using a command line interface. Deployment can be handled through an MDN or with a simple command. In terms of ease of use, this offers a substantial advantage over many other tools on the market ("night and day compared to other vendors", in the words of one member of the IR team).

With the sensors deployed, the team started pulling in relevant log files and used LimaCharlie's D&R rule customization feature to find endpoints that showed signs of compromise. The responders then took a closer look at suspicious endpoints in real time and, upon confirming the presence of IOCs, realized that they would have to perform full memory dumps for each of the affected machines.

As any incident responder knows, this can be a time-consuming and labor-intensive process. It often involves custom scripting work, as well as collecting and importing large data files — all before any detailed analysis can begin.

However, LimaCharlie's memory dumper feature significantly streamlined the task. As one of the responders recalled, "The memory dumps in LimaCharlie allowed us to skip and automate everything up to the 'doing the real work' step". In addition to simplifying the IR team's job, it also made things easier on their customers: "We didn't have to involve the local system administrators, or ship hard drives around".



Full containment in 24 hours with no downtime

Evidence of command and control (C&C) domains was found on a number of endpoints. Using LimaCharlie's global search feature, the team was quickly able to locate the same malicious domains on other machines.

It was imperative to lock down communication on the compromised network — both to prevent further malicious activity, and also to put a stop to the data exfiltration.

To do this, the responders installed LimaCharlie's SASE, LimaCharlie Net, on all POS systems as well as on the company's production machines. The IR team isolated the POS systems from everything else on the network, and restricted all other point-to-point traffic to business-critical communications only.

The breach was contained, and the retail company's normal business operations were able to continue without disruption while the IR team began the remediation process. As one of the responders remarked, this kind of operational continuity was clearly "a huge win for the customer".

As with earlier stages of the IR, LimaCharlie's "security infrastructure as a service" approach was critically important. According to a company official at the DFIR firm, this was the first time that they had actually been able to use a SASE during an IR engagement. "All of the other solutions require involving vendors, dealing with their sales team, and so on," they said, adding, "as with the rest of LimaCharlie, LimaCharlie Net is self-serve, so we were able to deploy it as easily as the EDR. We came in and went from zero to fully contained in a day".

> LimaCharlie Net is self-serve, so we were able to deploy it as easily as the EDR. We came in and went from zero to fully contained in a day.
>
> —Lead Security Operations

Trust won, business expanded

With the immediate threat contained, the IR team was able to create a custom remediation package based on information published by Microsoft. They deployed the package to the retail company's entire fleet using the LimaCharlie Payloads feature. Payloads allows arbitrary executables to be delivered and run on any endpoint that has a LimaCharlie sensor installed. It is particularly useful for performing remediation work at scale. As one responder commented, "Deploying with Payloads is super quick — it takes seconds".

The team also took steps to harden the retail company's network against future attacks. Using LimaCharlie tools, they set up real-time monitoring of Windows Event Logs and Windows Defender alerts. They also kept LimaCharlie Net — the SASE solution — installed on all POS systems, establishing a permanent private network for those critical endpoints.

The DFIR firm had originally been contracted in a purely incident response capacity. But by the end of the engagement, their relationship with the retail company had grown into a long-term MDR service offering.

A member of the leadership team says that LimaCharlie has been helpful in expanding business relationships with IR clients in this way. As they explained, "We're able to prove our value when it matters most. This 'land and expand' approach has been a really great way for us to build reliable revenue".

A model for future growth

The DFIR company's experience during this IR engagement highlights a major benefit of LimaCharlie's usage-based billing model: it can be an effective component of an overall business growth strategy. Since there are no pre-negotiated contracts or hig minimums (typical of other cybersecurity vendors), an IR team using LimaCharlie tools is free to take on new clients with confidence, and grow the relationship at their own pace.

Usage-based billing also means that LimaCharlie agents can be forward deployed onto a customer's less critical infrastructure at minimal cost. As a member of the DFIR company's sales team points out, this allows them to set up a true rapid-response capability — and to offer unbeatable service-level agreements: "If an incident occurs, we can simply turn the agents on. We have SLAs of 20 minutes with some of our customers — directly enabled by LimaCharlie's usage billing model".

Perhaps the biggest business benefit of LimaCharlie, says the leadership team at the DFIR company, is that they don't have to worry about competition from their own cybersecurity vendors:

"With LimaCharlie, we feel like we own the relationship with the customer. We don't have a vendor breathing down our neck just waiting to swoop in when the IR is over to convert them to their MDR customer — when we're trying to do the same thing!"

LimaCharlie's Christopher Luft says that this is all part of the company's overall vision: "We're trying to change how cybersecurity tools and infrastructure are delivered: self-serve onboarding; transparent, usage-based pricing; and an open API. Because at the end of the day, we want to put the full power of LimaCharlie where it belongs — in the hands of our users".

To learn more about LimaCharlie,
try it out for free or book a demo today.

Book a Demo: calendly.com/demo-lc
Sign Up: app.limacharlie.io/signup

> We have SLAs of 20 minutes with some of our customers — directly enabled by LimaCharlie's usage billing model.
>
> Sales Manager