A brief introduction to Latacora

Latacora bootstraps security practices for startups.

Security is a complex, multifaceted problem: startups don't need a "security person" as much as they need application security assessment work on Monday, guidance from a Cloud security person on Tuesday, a third party risk management security review on Wednesday, someone who can handle compliance on Thursday and an IT security expert on Friday—oh, and also ongoing security monitoring throughout the week.

Instead of spending an unbounded amount of time trying to hire a unicorn who is great at every aspect of security but can't get a good night's sleep or take a vacation, you engage with us. We have a diverse team of experts pre-equipped with processes and power tools covering an enormous range of security capabilities. That lets you de-risk and accelerate acquiring security talent while assuring you have every security capability you're likely to need now or a year from now.

How we work with customers

All Latacora engagements begin with us getting to know your overall security posture. We'll generate a set of Security Architecture and Maturity recommendations that cover application, cloud, deployment, and corporate security.

Smaller companies in our "Jumpstart" model, or those whose security stance is less mature, will proceed in a more bespoke manner based on mutually agreed-upon priorities to get their security practices in a proper state. When security practices look healthy and robust, we'll discuss with those clients when they're ready to proceed with more formal assessments.

More mature organizations in our "Retained" model who meet general maturity expectations or who have specific compliance requirements will then proceed into performing initial security assessments across application, cloud, network perimeter, and various aspects of corporate and deployment security.

Latacora is around for the long haul. Our median engagement length is around 2.5 years and trending up. Compared to a traditional hire, we tend to stick around longer. Also, we come pre-equipped and ready to go; we can engage sooner than a traditional hire. We've started with companies as tiny as 3 people and have had more than one client go public.

Security Architecture Review

Latacora's Security Architecture Review is a holistic look at your organization's security risks, covering as broad a spectrum of information security as possible. The goal is to produce a broad understanding of the organization's risk profile. These documents allow us to collaboratively drive priorities, based on the risks presented by your current security stance, rather than being solely based on vulnerabilities or hunches.

The output of this review will be a security maturity assessment and a priority-ranked list of risks, with guidelines for remediation. We'll suggest activities with the highest return on investment. We'll also identify areas that require deeper and more comprehensive audits.

This review will cover the most common risks but is not intended to be comprehensive. It will identify foundational risks limiting your ability to build a secure system, deploy to a safe cloud, or feel comfortable about your employees in an increasingly complex remote working environment. The goal here isn't to enumerate every potential flaw, or to prevent errors in implementation. We will, however, identify gaps that the remediation could significantly reduce the risks your company faces.

Jumpstart Services

In all Latacora engagements, there's a set of activities we plan to do on an ongoing basis. They're most of what a typical startup wants a security team to do, working closely with your engineering teams.

Advisory services and design review

We staff a channel on your Slack. We provide ongoing, all-day "office hours" for questions and security concerns.

Our clients have unmetered access to our calendar to set up design discussions and review meetings (or, for that matter, any other kind of meeting we can be helpful in). We're particularly interested in getting involved early in the security design process for new features and projects. We have extensive experience shipping commercial systems and operating businesses: we're good at these kinds of meetings.

We're also comfortable documenting security designs, evaluating available open-source and commercial solutions, and monitoring tickets to track progress.

We have a team of expert Security Architects who are also skilled engineers. Our customers have this team of architects available to them for design doc reviews, RFCs, and broad conversations about how to even start architecting a solution. Our Security Architects have worked across industries and collaborate with our other experts to help you create the best solutions.

Compliance

If SOC2 is on your roadmap, we're here to help! Substantially all of our clients either have a SOC2 or are in the process of getting one, and we're a key partner in making that happen.

Outside of SOC2, we have clients in various regulated and compliance-driven verticals. We've helped fintechs, healthcare companies, medical device companies, literal banks, and drug testing companies achieve compliance and close deals. We've helped SaaS companies with complex integrations and mounds of data figure out how to handle privacy regulations like GDPR and CCPA. Having gone through this gauntlet a bunch, we're great at translating audit requirements into actionable approaches and knowing what's standard industry practice (and what isn't). We're also happy to coach you on how you should talk to your auditors about your systems, policies, and compensating controls.

For SOC2, we'll help figure out where you're at process wise, and help take temperature on your SOC2 readiness. If you have timelines for SOC2 in mind, we'll also help figure out how realistic that is.

Our Jumpstart customers may be starting with no policies or procedures yet. We'll help you establish a lightweight but effective compliance practice built for where you are now, and that can grow as you do. For our Retained customers, we'll make sure what you have is accurate, sufficient, and that the evidence you need to pass SOC2 or similar is being collected.

Cloud monitoring

Latacora will continuously monitor AWS cloud infrastructure configurations and activity through a combination of internal tooling that performs the following:

- Regular snapshots of discovered resource configurations
- Rule-based analysis of configurations
- Rule-based analysis of activity via CloudTrail events

Throughout the life of the engagement, Latacora will keep an eye out for scenarios that indicate risk. This includes:

- Overly permissive resource configurations, e.g. Publicly accessible S3 Buckets, RDS Instances, Security Groups, and others
- IAM configurations that could lead to privilege escalation or violate best practices, e.g. broad access policies using wildcards, inline policy use, MFA not enabled
- Anomalies in CloudTrail logs indicating abuse of any AWS resources
- Secrets stored insecurely in AWS provisioning tools

Latacora can also guide as needed for the remediation of existing resources and guidance for new architecture plans. Similar monitoring is also available for other cloud providers such as GCP.

Network perimeter monitoring

We run what amounts to a continuous low-grade network penetration test for all our clients, which includes routine scheduled light-touch scans and collecting open-source intelligence indicators.

Security Information and Event Management (SIEM)

In addition to our normal cloud monitoring, we can collect and analyze your infrastructure logs via our Panther SIEM offering.

The combination of our own cloud monitoring technology and Panther's capabilities give you insight to security events across your organization. Panther provides multiple out-of- the-box detections aligned with CIS and MITRE frameworks as well the ability to write custom detections.

Our Panther setup is designed to be simple to port ownership to you if you want to take it over in the future.

Latacora is also actively piloting an IR retainer program built on top of these capabilities. Please let us know if you're interested in adding that pilot program to your SoW.

Patch Triage

Like any in-house security team, we are monitoring various channels for vulnerability announcements. We will feed that information back to your team to let you know if we become aware of an issue that may affect you.

Security Issue Tracking

No matter where issues come from, be it our network perimeter monitoring, a new discovery made during a routine code change review, or a bug bounty submission, if it is relevant to security, we'll be tracking it internally and following up on it during our check-in meetings. Part of our job will be ensuring issues aren't lost in the shuffle.

Penetration Testing and Assessments

Our Jumpstart customers often approach Latacora due to a prospective client requiring third-party penetration testing and similar assessment work. Latacora is happy to do these services on an ad hoc basis to meet contractual or compliance obligations; we'll need advance notice to ensure these things happen according to your needs, so please let us know what you're thinking, and we can discuss what needs to be added to your statement of work so we can perform those assessments for you.

Retained Services

In addition to the services offered in our Jumpstart offering, companies engaged in the Latacora Retained offering follow their Security Architecture and Maturity Review with initial assessment projects in which we evaluate the key technical areas of operation for startups:

- Application Security
- Cloud Security
- Network Perimeter
- Corporate Security

Initial assessment work will typically cover the areas of greatest risk based on our Security Architecture Review. We'll use this initial set of assessments to generate formal deliverables of the sort auditors or potential customers expect to see.

As we perform additional tests, we'll update those documents so they provide information about the testing performed over the past 12 months - evidence of a serious ongoing security testing program that auditors and potential customers love to see.

Assessments

Latacora performs regular assessment work for Retained clients. These often

include formal reports and letters of engagement that your auditors and customers will likely want to see.

Rather than perform monolithic tests and one-off reports, we'll generate documents demonstrating an active security assessment *program* instead of a performative checkbox approach.

There will be a number of tests we undertake across various areas based on the risks identified in the Security Architecture review. We'll use these as the starting point for generating formal assessment documents. Over the coming months, as we perform additional assessment work, we'll update these documents so interested parties will see all of the work being done, and not just a two-week snapshot in time.

We'll be watching for areas we think merit additional testing, and we'd appreciate it if you came to us with the same. Our assessments cover everything from your network, application, cloud, Google Workspace, GitHub, new features, etc.

Assessments will cover the typical topics when you think about security like OWASP Top 10 and other common vulnerabilities, but will also cover topics such as the principle of least privilege, IAM policies, plug-ins and extensions, and other checks specific to your industry.

Application Security

Outside of our application assessment work, our Application Engineers are here to help you with code review and training. Most importantly, Latacora wants to help you incorporate security throughout your SDLC, and come equipped with the tooling and processes to help you do so.

Code Review

We'll regularly ping your engineering team to make sure they know that they can tag us whenever they want to get a security review. The requester will only have to create a pull request and send us a link to review . We'll review and comment on it.

Corporate Security

The corporate security team helps tackle key security initiatives identified through our initial review. Every organization's needs vary based on its size and the risks it faces, and the corporate security team works with customers to find solutions that take our customer's specific needs into account.

As part of the ongoing relationship with Latacora, the Corporate Security team can help with a variety of activities. We often advise customers on key IT questions like which MDM solutions to use, laptop security baselines, and how best to deal with the risk of personal devices for work.

Managing third-party service risk is a common challenge for our customers. Latacora's corporate security team is available to help build a program to begin taming these risks and perform reviews for high-risk services.

Helping customers develop sound security policies and corresponding procedures is another area where we're happy to help, especially in preparation for compliance audits.

Sales enablement

Many of our customers have found our Vendor Security Questionnaire (VSQ) service invaluable for sales enablement - we're happy to help our clients streamline this process, and enable their sales teams to quickly and accurately respond to these requests.

Hiring

What about when your team needs additional internal security expertise? We're designed to stick around with our customers long-term, but not at the expense of helping you build your own team when it makes sense. We'll be there to help identify what in-house security expertise you need the most, craft a JD, figure out how to vet the candidate, run work sample tests with them to see how capable they are, figure out how to interview - all of the stuff you'd expect your security team to help you do!

Engagement day-to-day

Staffing

Latacora isn't a staff augmentation firm: we don't select a lucky member of our team and designate them as your new security do-everything-person. We don't believe one person can address the needs of even a small organization when it comes to security. No matter how talented our team members are in their area of expertise, the best cloud security person probably isn't going to be the best possible resource to answer your questions about cryptography, whether a policy is necessary and sufficient for SOC2, or specific concerns around Android Intents.

Every client has an assigned team who'll act as their primary subject matter experts: multiple Latacora staff will be regularly engaged with you across application, cloud and corporate security, compliance and security architecture. Each client team is made-up of "squads" from our delivery teams to not have a single point of failure for (we like our team to use their vacation), When a highly specialized need arises (cryptography, for example) we'll pull the right resource in from our organization to work alongside the squad members with the most pertinent institutional knowledge to address them.

Project Management

Every Latacora client has an assigned project manager, who will work with you and our squad members to keep everyone apprised of what's going on with your engagement, provide updates on things we're working on for you, and make sure we're kept abreast of changes on your end. Our PMs will engage with you often. This will typically be through meeting on a regular basis and communicating on slack. They are your "go-to" person as they know how to get your requests in front of the right internal personnel and will be able to update you on the status of our work!

What don't we do?

We're wary of directly modifying your infrastructure or writing code for your projects. We're trying to teach you how to fish. While we might be in the boat and holding your hands as you cast the reel, our goal is to weave security through your organization, and that can't happen if we're just fixing bugs in isolation.