Beyond Automated Cloud Security

September 30, 2022

Senior Cloud Security Consultant

Alon's IT career spans academic, start-up, and corporate environments. He has deep experience in a wide variety of specialties including cloud security, security operations and intelligence, software development, platform and reporting automations, and mixed-method analysis.

Submitted by Alon Diamant-Cohen on 30, Sep 2022
Beyond Automated Cloud Security

Traditionally, when enterprises want to strengthen or evaluate their cloud security, business priorities and concerns such as product launch dates and compliance will define the deadlines. There’s pressure to rapidly understand and address critical risks to improve your overall cloud security posture. This frequently drives teams to deliver *only* the exact results requested as quickly as possible.

However, that approach to cloud security delivers short-term results at the expense of long-term benefits. To produce meaningful insights, you need to analyze the context behind the original request. Doing so helps you discover the pain points motivating the request along with the organizational context and history that brought about this moment. You can use that information to frame cloud security insights in a way that both resonates with the requestor’s issues and aligns with the enterprise’s long-term strategy.

The Tech Trap

Frequently, security practitioners fall into the trap of trying to automate everything—jumping straight into the *how* without contemplating the *why*. Reviewing cloud environments for important technical controls such as “S3 data encrypted at rest” is important. However, we believe that such technology-based controls are only part of the security puzzle. You also need to understand why things are configured as they are. Additionally, an overreliance on technology-based controls can lead an organization to automate itself into complacency.

Numerous security solutions purport to do parts or all the assessment work for you, such as Cloud Security Posture Management (CSPM), Cloud Infrastructure Entitlement Manager (CIEM), and Audit Preparedness. In our experience, however, nothing replaces the legwork of asking the questions yourself, hearing the answers, and processing them alongside any technology-driven findings.

Deep Discovery

At Stratascale, we take a measured approach to cloud security. Our proprietary evaluation framework maintains a balance between automatable and non-automatable controls to guarantee a thorough evaluation. We get to know and understand the context driving our customers’ security needs. Such context helps us frame our findings to align with our customers’ historical pain points and deliver more long-term strategic value.

A few specific principles driving our discovery approach include:

- **Interviewing key stakeholders**

  When it comes to gathering insights, email and webforms are no match for in-person interviews. Further, conducting meaningful interviews that feel like friendly discussions rather than interrogations is a skill that requires practice and study to perfect. An experienced interviewer can extract rich information by listening closely and acting on seemingly subjective context, such as slight physical reactions, stray comments, or mention of things like a document that “might be related.”

- **Reviewing published documents and processes**

  An organization’s published documents and processes, even those only for internal use, are the official guides that many employees use to execute strategic company goals. We head off potential missteps by identifying any conflicts between interviewees description of a process vs their description in published documents.

- **Understanding the history**

  When evaluating an organization’s needs, it’s easy to get lost in characterizing the current situation. History tends to repeat itself, though. By studying an organization’s history, you often find past examples of similar challenges and discover capabilities you can leverage in confronting comparable challenges.

A Complete Characterization

By gathering intel about technology-driven controls and context from stakeholder interviews, you gain a more complete characterization of the organization behind the cloud security needs. Understanding the motivations and history that led to this point can help you frame any security vulnerabilities as well as recommendations for remediation.

What’s Next?

When delivering a cloud security assessment, make sure your reporting includes meaningful recommendations—not simply a listing of all the problems that you found. Organizations derive maximum value when recommendations account for specific context and lessons from previous attempts. These insights help to ensure an efficient and smooth implementation of stronger cloud security measures.