Horangi and GoJek - Hand-in-Hand Cloud Security for Your Safety from End-to-End

gojek

With competitors snapping on their heels in a highly competitive ride-hailing and delivery services market that has seen unprecedented growth because of the Covid-19 pandemic, keeping 36.3 million monthly active users happy depends very much on the ease and speed of GoJek's services and how the company can ensure the safety of their customers' data at every touchpoint of the customer's journey.

Founded in 2010 with the aim of providing solutions to Jakarta's perennial traffic problems, Gojek started as a call center with a fleet of only 20 motorcycle-taxi (ojek) drivers.

Today, Gojek is a "Super App" — a one-stop platform offering more than 20 services that connect users with more than 2 million registered driver-partners and 500,000 GoFood merchants in Indonesia, Vietnam, Singapore, Thailand, and the Philippines.

As of June 2020, it has about 170 million users throughout Southeast Asia and is the only company in Southeast Asia that is included in Fortune's 50 Companies That Changed the World in 2017 and 2019.

SERVICES

- CISO-as-a-Service

OVERVIEW

Horangi has had a long-running relationship with Gojek, performing penetration testing and various other security assessments, when Horangi was engaged to assist with a new type of service: To create incident response playbooks for Gojek's internal IT helpdesk.

After looking further into this need, Horangi observed that the company's IT helpdesk was requesting playbooks as they did not have personnel with cybersecurity backgrounds to field security incident escalations.

Horangi saw that fulfilling the request would help the IT helpdesk, but identified that developing such a capability apart from the IT helpdesk may prove to be a more effective long-term solution. A specific computer security incident management capability within the organization was then proposed, to which the client agreed.

APPROACH

ASSESS

Before jumping into developing an incident management capability, Horangi collected information on the existing ways that the organization had already established for identifying security incidents and working through them to resolution. Assessment of the gathered information-enabled Horangi to identify areas where processes could be standardized and workflows could be consolidated in order to streamline incident management.

CONSOLIDATE

Understanding that an organization can only respond to security incidents effectively when they have a full picture of what is going on in their organization, Horangi set off to consolidate all the different security incident workflows so that there was one central location for incidents to flow, ensuring that no incidents fall between the cracks. This meant developing new processes, producing new guides and workflows, and training personnel, system owners, and end-users in these new processes to escalate security incidents when they occur in the future. These enhancements also empowered the organization to record data on these incidents for advanced metrics that were previously difficult to measure such as attack vector classification and response time tracking.

DEVELOP

Now that there was a standardized, coherent flow for security incidents within the organization, Horangi set to work on creating a team that could oversee the life cycle of computer security incidents from creation to closure: A Computer Security Incident Response Team (CSIRT).

Horangi developed content such as playbooks, roles and responsibilities, worksheets, documentation, and other tools for the daily operations of a CSIRT. Horangi then wrote Job Descriptions and helped the organization to recruit qualified personnel to man this newly-established team, and when they were onboarded, trained said personnel.

Using an industry-accepted framework for CSIRT services, Horangi worked with the organization to build out the CSIRT's capabilities in a phased manner starting from a structured approach to accepting, triaging, and analyzing security escalations, working their way up to coordinating cross-team collaboration on investigating open incidents, to developing communication plans and remediation plans for incidents, as well as leveraging available data to provide metrics and regular reporting on CSIRT observations and efficacy.

CONCLUSION

Today, Gojek has the first line of defense against security incidents as they crop up and is fully capable of handling and tracking the incidents to swift resolution and closure. This team works hand-in-hand with Gojek's existing IT helpdesk, system owners, end-users, and vendors to ensure all security incidents are handled by qualified personnel.