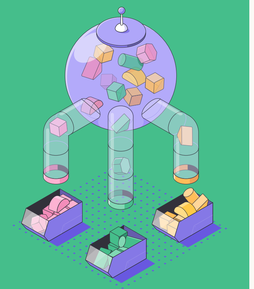
Canva + tines

CUSTOMER CASE STUDY

Improving Canva's security detections, response, and compliance

Phishing can be a serious threat to a company's security, and protecting against these attacks is just one way we use Tines. When a user reports a suspicious email, Tines extracts data from the messages, such as URLs and file attachments. It then passes them to a number of scanning tools such as antivirus software, and sandboxing tools that automatically test links and files to determine what they do.

Tines then takes the results of these tests and adds them to our ticketing system for a security analyst to pick up.



CUSTOMER CASE STUDY

Canva + tines

Canva & Tines

The Challenge

As a creative playground for established and emerging brands to experiment with and build visual identities privately, Canva takes security very seriously and trust is at the center of what they do. Their products, processes, and systems are designed to protect their users and their users' data as their growth continues to accelerate.

Canva has invested heavily in its security in recent years. They run a tight ship of manual and automated checks for security issues. They also operate a bug bounty program that provides ways for security researchers to notify them of vulnerabilities in their products and environments.

In addition to handling alerts, the team's workload includes performing general security sanitization work to ensure they have best practices in place for their sizable internal infrastructure and implementing tooling improvements.

Why Tines

Canva's incident response team needs a very flexible, programmable interface that allows them to send alerts to various locations without having to write something large and unwieldy themselves.

The team has grown significantly over the past year, and they chose Tines to help scale up and improve their security detections and their response work.

About Canva

Canva is an online design and publishing tool with a mission to empower everyone to design anything and publish anywhere. Users can create their social media graphics and marketing materials using free templates to develop everything from logos to Instagram posts.

- Founded in 2013
- Customers in 190 countries
- Over 1500 employees
- 55 million monthly active users
- Over 6 billion designs made to date

Key Benefits

Enterprise-grade
All the compliance and features you need.

Runs anywhere
From our managed cloud to on-premises.

Flexible
Our customers automate dozens of use cases.

Robust
Fault-tolerant, with monitoring and alerting built in.

Community Edition
Start on our generous always-free plan.

CUSTOMER CASE STUDY

Canva + tines

Mike's Story

Mike Fountandez, Senior Security Engineer at Canva, explains how Tines has helped the company scale up its security efforts and maintain a sound compliance posture.

While we're not a new security team, we're growing and changing significantly. We wanted to spend as little development time as we could on getting the plumbing working; our focus was to scale up and improve our security detections and our response work. We needed something that could help us do that quickly, and I think Tines has done that very well.

We manage a number of permissions through groups in our SSO provider, and in order to join those groups, there is a request process. In order to ensure that teams were not able to bypass our request process, we wrote an alert in our SIEM platform which triggered a webhook in Tines. In Tines, we extract the user ID and the group ID and have Tines automatically send a request to our SSO provider to remove the employee from that group if the proper process wasn't followed. The net effect is that our employees can be protected while still getting the access they require to do their jobs. We also reach out to them automatically via chatbot and ensure they know about the proper process so they can take the correct action next time.

Another problem we're solving is employee notification. If an employee did something potentially concerning, a member of the security team would normally reach out to them personally and get more context. In order to alleviate some of our operational load, we've created a chatbot that is in the flow of several of our Tines Stories. It receives alerts from a variety of different sources, and each has a template to allow us to have a chatbot reach out to the employee and say, 'Hey, we saw X activity; was this you?'. The employee can send us a response so we can decide whether we need to treat this as an incident or mark it as a false positive.

We also integrate Tines closely with our incident case management system. Let's say the chatbot comes back with a response from an employee saying, 'Nope, I didn't perform this action.' In that case, we're really excited to be able to format and send case information over to our case management system for analysis, and to notify the team in a variety of locations. That's one of our biggest use cases to grow in Tines: building alert context, doing enrichment, and creating cases automatically for investigation.

Tines has been a refreshingly reliable platform to use, and we really appreciate the collaborative approach the Tines team has with us; we have never had an issue with the reliability of the Tines platform, and they are quick to respond to feature requests. I think Tines puts out solid products that are tested well before launch.

This is my first time doing event routing, and I've found Tines pretty straightforward to use. Having a product that works well out of the box allows us to be flexible and agile, which is very impactful.

As with any security team, there are some people that are a lot more skilled on the infrastructure side, some that are more skilled at threat hunting and threat intel, and others that are more core incident response. Tines is a tool that all of us have been able to use to move the needle forward.

A major challenge in security is ensuring that you don't bury yourself under alerts; it's critical to filter false positives out before humans get involved. Having a tool like Tines helps us to be ready to onboard the next alert by empowering us to filter false positives, freeing up our time for more valuable tasks.

It's nice that you can build context as you go, in terms of adding fields and building logic in Tines. It seems like an easy platform to both build through and test through; once you can get any data into it for an alert, you can iterate quickly by replaying those events and making sure your workflow works well.

We have a large use case for AWS event triage, namely Guard Duty alerts. Guard Duty can be high volume; we have a Story that does general triage and sanity checking before we pass alerts off to our case management tool for subsequent action by a human.

I've been on teams where the concept of runbook automation — where you can automate established processes to free up responders for more critical parts of the workflow — has been a pipe dream. Tines is a flexible platform that helps us achieve that goal in a simple and effective way. While we're not there yet, I can see the light at the end of the tunnel.

I think automation is critical to the security of an organization, and anything that makes the work around the infrastructure side of it easier will actually make it real. It's 100% necessary.

Mike Fountandez
Senior Security Engineer, Canva

Ready to get started?

tines

Create a free Community Edition account now and start automating. You can also contact us if you'd like a demo or discuss one of our paid plans.

tines.com
hello@tines.com
calendly.com/talk-to-tines

Trusted by the world's leading security teams

auth0 | box | Canva | coinbase | McKESSON

OpenTable | SOPHOS | Informatica