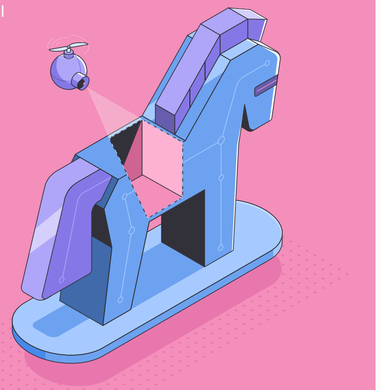
USE CASE

tines

Automating Phishing Response

Flexible and intuitive, Tines enables customers to automate the essential manual tasks that analysts routinely perform when responding to user-reported phishing emails.



Trusted by the world's leading security teams

auth0 | box | Canva | coinbase | MCKESSON

OpenTable | SOPHOS | Informatica

USE CASE

tines

Phishing emails have become the most common way of gaining sensitive information and distributing malicious programs like ransomware. As much as 25% of a security analyst's time is spent chasing false positives.

A secure, stable, and agile automation solution, Tines helps manage alerts and execute appropriate responses at scale. By automating the eight tasks listed below, customers can respond faster, take action automatically, and streamline their internal processes, making them better prepared for high-priority incidents.

Leverage customizable templates and easy-to-configure Actions within Tines to:

1. Read emails from your abuse inbox.
2. Create tickets in Case Management tools or systems of record.
3. Extract observables and context from attachments, email body, headers, etc.
4. Analyze files or links dynamically in any malware sandbox.
5. Connect to any threat intelligence sources to enrich indicators.
6. Communicate with reporter and internal teams via Slack, Microsoft Teams, email, etc.
7. Take action quickly in any security tool using 'prompts.
8. Easily customize and iterate automation Stories and processes for your environment.

Key Benefits

Automate
Remove bottlenecks and manage large volume workflows by automating inbox scanning, data collection, enrichment, and notifications.

Reduce Duplication & Errors
Save time investigating duplicate events and false positives, and take action in your tools.

Streamline Actions
Streamline and standardize your process of responding and taking action on results.

Numbers say it all
Demonstrate time-savings and return on investment utilizing Tines' metrics report.

> We've found that just one of our earliest implementations frees up 1.5 analysts per week. That's a lot of human hours that we can put into more complicated and professionally rewarding work.

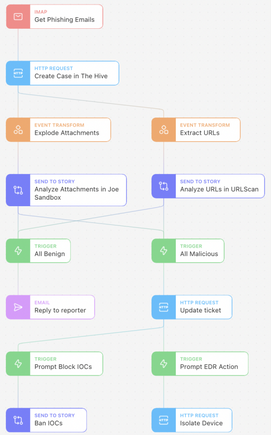
John McSweeney,
McKesson, Director of Defense

MCKESSON

USE CASE

tines

Story Example



Getting Started

1. **Estimated Deployment Time**
   2 hours

2. **Required Tools**
   Email, Case Management (e.g.JIRA / ServiceNow), IOC Analysis Tools (e.g.URLScan, Joe Sandbox, VMRay, Hybrid Analysis)

3. **Optional Tools**
   EDR (e.g. CrowdStrike, SentinelOne), Collaboration Tool (e.g. Microsoft Teams, Slack), Threat Intel Sources (e.g. AbuseIP, DB, URLScan)

Ready to get started?

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