



# ACME Anvils Ticketing System

10.16.2023

—

SOC Team

ACME Anvils

Denver, Colorado

## Overview

The SOC Team here at ACME Anvils has been notified that there is still an excessive amount of IT and Security issues that hinder the company. It is our job as the SOC Team to ensure these issues are resolved adequately and in a timely fashion. ACME Anvils is in need of a new ticketing system in order to maintain vigilant oversight and allow for better resolution of outstanding issues. After thorough analysis, we have narrowed it down to one ticketing system we think would benefit ACME Anvils the most.


## Goals

- Suggest possible ticketing systems to enhance IT and Security response
- State the resources and architecture needed for such ticketing systems
- Provide details on the budget expenses on such ticketing systems

## TheHive 5

Created by StrangeBee, TheHive 5 provides a comprehensive solution for security incident response and case management built for organizations of all sizes. TheHive 5 is a scalable Security Incident Response Platform tightly integrated with MISP (Malware Information Sharing Platform) designed to make life easier for SOCs, CERTs, CSIRTs, and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly. Key features of TheHive 5 include:

- Collaborative multitenancy
- Advanced User management
- Case management
- Alert management
- Metrics and dashboards
- MISP Integration
- MITRE ATT&CK knowledge base Integration



StrangeBee produces two different services for TheHive 5, one being on premises, and the other being Software as a Service (SaaS). The on-prem solution ranges from free to \$28,000 per year, (free being a community version) while the cloud based solution ranges from \$45,000 to \$55,500. They also provide custom pricing based upon an infrastructure tailored to your organization's needs. Organizations can choose a plan that fits their requirements as there are certain features that are included within certain packages. Each plan allows up to five users and one organization on the platform.

Within the platform, SOC and CERT analysts can collaborate on investigations simultaneously. Due to the built in live stream, real time information pertaining to new or existing cases, tasks, observables, or IOC's is available to all team members. Cases and associated tasks can be created using a simple yet powerful template engine. You may add metrics and custom fields to your templates to drive your team's activity, identify the type of investigations that take significant time and seek to automate tedious tasks through dynamic dashboards. Analysts can define notification rules to invoke Webhooks, send emails, Slack and Mattermost messages or call custom HTTP requests. TheHive allows full access for users to documented APIs to implement workflows or develop any automated scripts using TheHive data. For each case, analysts can obtain a well-organized synopsis of the incident's progression, tracing it from its initial detection through to the resolution and recovery phases. You can opt to display a detailed timeline specifically focused on the sequence of events related to the cyberattack or alternatively, present a comprehensive view of the entire incident response process.

## Conclusion

TheHive 5 will allow the team here at ACME Anvils to sustain proper supervision while enabling improved problem solving for unresolved issues. We as the SOC Team want nothing but the best for ACME Anvils, and we believe TheHive 5 is the most comprehensive solution to our IT and Security issues that continue to hinder the organizations IT and Security posture.