Coalfire ThreadFix SaaS

Service Description

This Service Description describes Coalfire's Threadfix SaaS ("Service"). All capitalized terms in this description have the meaning defined in the Agreement or in the Definitions section.

This Service Description, with any attachments included by reference, is part of and incorporated into Client's manually or digitally-signed agreement with Coalfire which reasonably governs the use of the Service, or if no signed agreement exists, the Service Agreement found at: https://www.coalfire.com/agreements/sa (together, the "Agreement").

Table of Contents

1: Technical/Business Functionality and Capabilities

Service Overview

The ThreadFix™ Service is a web-based, Software-as-a-Service application and vulnerability management platform designed to allow Clients to manage their application vulnerability assessment, scanning, and remediation programs. During the Subscription Term, Client may use the Service in accordance with the Agreement.

Service Features

- Client can access the Service through a self-service online portal ("Portal"). Client may configure and manage the Service, and view dashboards, through the Portal
- The Service is managed on a business hours basis and is monitored for hardware availability, service capacity, and network resource utilization. The Service is regularly monitored for service level compliance and adjustments are made as needed.
- The Service includes the following capabilities: Integration with industry leading SAST, DAST, SCA, and IAST scanning technologies, developer defect tracking tools, automated ingestion, policy evaluation, and alerting.
- Client may configure ingestion automation, create custom vulnerability policies and alerting, upload and manage vulnerability scan results and application assessment results, and automate the creation of and reporting on developer defects based on client criteria.

2: Client Responsibilities

Coalfire can only perform the Service if Client provides required information or performs required actions, otherwise performance of the Service may be delayed, impaired or prevented, and Client may lose eligibility for any Service Level Agreement.

- Setup Enablement: Client must provide information required for Coalfire to begin providing the Service.
- Adequate Client Personnel: Client must provide adequate personnel to assist Coalfire in delivery of the Service.
- Client must acquire and maintain all required licenses for third party tools that the Client wishes to integrate with the Service.
- Client Configurations vs. Default Settings: Client must configure the features of the Service through the Portal, if applicable, or default settings will apply. In some cases, default settings do not exist, and no Service will be provided until Client chooses a setting. Configuration and use of the Service are entirely in Client's control, therefore, Coalfire is not liable for Client's use of the Service, nor liable for any civil or criminal liability that may be incurred by Client as a result of the operation of the Service.
- The Service supports Integrations defined here: https://www.coalfire.com/solutions/threadfix/integrations

3: Entitlement and Subscription Information

Meter Metrics

The Service is available under the following Meter as specified in the Order Confirmation:

• "**Application**" means each code repository or set of code repositories that Client designates as a unique asset to be scanned, assessed, and/or tracked for vulnerability management purposes and for which Client has received scan or assessment data.

4: Additional Terms and Disclosures

A. The Service is currently offered in the following development stages and Client is given access as part of a selected test group in each stage. Client will be notified in writing of the applicable stage and must notify Coalfire in writing if it requests to migrate to a different stage.

- Beta: This offering is at no charge for current Clients of the on-premises software version of ThreadFix 2.x or 3.x. Client may use the Service in a production environment as part of a test group to allow Client and Coalfire to obtain real-time results and feedback on the Service. Technical Support is available from 9:00 am to 5:00 pm US Central Time. Technical Support Issues may require downtime to investigate and resolve. Service Level Agreements are not available in the Beta stage. Requests for account creation or migration for unique environments require manual action and will be performed as commercially reasonable in the order requests are received. Coalfire does not offer any warranty, indemnification, nor accept any liability for Client's use of the Service in this development stage and Client uses this version at its own risk.
- Limited Availability: This is a paid Service and includes all of the features and terms of the Beta stage. Additionally, Client may purchase automated account creation Services.

B. Invoicing: Client will be invoiced on a monthly or annual basis as defined in the Order Confirmation. Clients who are invoiced monthly will be invoiced for the highest number of Applications that used the Service within the billing cycle. Clients who are invoice annually will be invoiced for any overage in the maximum allowed Applications in a separate true-up invoice at renewal or the end of the Subscription Term.

5: Client Assistance and Technical Support

Client Assistance

Coalfire will provide the following assistance as part of the Service, during regional business hours:

- Receive and process orders for implementation of the Service
- Receive and process requests for permitted modifications to Service features; and
- Respond to billing and invoicing questions

Technical Support

If Coalfire is providing Technical Support to Client, Technical Support is included as part of the Service as specified below. If Technical Support is being provided by a reseller, this section does not apply.

- Support is available during Normal Business Hours to assist Client with configuration of the Service features and to resolve reported problems with the Service.
- Once a severity level is assigned to Client's submission for Support, Coalfire will make every reasonable effort to respond per the response targets defined in the table below during Normal Business Hours.
- The Support Response and Update Targets are attainable during normal service operations and do not apply during Maintenance to the Service and/or supporting infrastructure as described in the Maintenance section below.
- Issues originating from Client actions or requiring the actions of other service providers are beyond the control of Coalfire and as these issues are specifically excluded from this Support commitment. Response and Update targets are not commitments for resolution.

Problem Severity	Support Response Target	Support Update Target
Severity 1: A problem has occurred where no workaround is immediately available in one of the following situations: (i) Customer's production server or other mission critical system is down or has had a substantial loss of service; or (ii) a substantial portion of Customer's mission critical data is at a significant risk of loss or corruption.	8 Hours	Every 48 Hours
Severity 2: A problem has occurred where a major functionality is severely impaired. Customer's operations can continue in a restricted fashion, however long-term productivity might be adversely affected.	2 Days	Every 4 Days
Severity 3: A problem has occurred with a limited adverse effect on Customer's business operations.	4 Days	1 Time / Week

Maintenance to the Service and/or supporting Service Infrastructure

Coalfire must perform maintenance from time to time. The following applies to such maintenance:

- **Planned Maintenance:** Planned Maintenance means scheduled maintenance periods during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. During Planned Maintenance, Service may be diverted to sections of the Service Infrastructure not undergoing maintenance which may result in no disruption of the Service. For Planned Maintenance, Coalfire will provide seven (7) calendar days' notification in writing.
- **Unplanned Maintenance**: Unplanned Maintenance means scheduled maintenance periods that do not allow for seven (7) days notification and during which Service may be disrupted or prevented due to non-availability of the Service Infrastructure. Coalfire will provide a minimum of one (1) calendar day notification in writing. During Unplanned Maintenance, Service may be diverted to sections of the Infrastructure not undergoing maintenance which may result in no disruption of the Service. At times Coalfire will perform Emergency Maintenance. Emergency Maintenance is defined as maintenance that must be implemented as quickly as possible to resolve or prevent a major incident. Notification of Emergency Maintenance will be provided as soon as practicable.

6: Definitions

Administrator	means Client's designated personnel to manage the Service on behalf of Client.
Service Infrastructure	means Coalfire or licensor technology and intellectual property used to provide the Services.
"Software as a Service" and "SaaS"	means a term limited web-based application provided by Company to Customer. The Software is not perpetually licensed to Customer.

Exhibit A: Service Level Agreement

1.0 GENERAL

These Service Level Agreements ("SLA(s)") apply to the Online Service that is the subject matter of this Service Description only. If Coalfire does not achieve these SLA(s), then Client may be eligible to receive a Service Credit. Service Credits are Client's sole and exclusive remedy and are Coalfire's sole and exclusive liability for breach of the SLA.

2.0 SERVICE LEVEL AGREEMENT(S)

a. **Availability.** Availability is the amount of time that the Service is operational in minutes, expressed as a percentage per calendar month, excluding Excused Outages. The availability calculation is based on the entire calendar month regardless of the Service start date.

Availability SLA	**99.0%**

3.0 AVAILABILITY CALCULATION

Availability is calculated as a percentage of the total minutes per calendar month as follows:

(Total Minutes – Excused Outages – Non-Excused Outages) / (Total Minutes – Excused Outages) x 100 = Availability %.

4.0 SERVICE CREDIT

If a claim is made and validated, a Service Credit will be applied to Client's account.

Coalfire will provide a Service Credit equal to two (2) days of additional service for each 1 hour or part thereof (aggregated) that the service is not available in a single 24-hour period, subject to a maximum of seven (7) calendar days for all incidents occurring during that 24-hour period. A Client may only receive up to twenty-eight (28) days maximum, for up to four (4) Service Credits, over twelve (12) months. The maximum is a total for all claims made in that twelve (12) month period.

Service Credits:

- May not be transferred or applied to any other Coalfire Online Service, even if within the same account.
- Are the only remedy available, even if Client is not renewing for a subsequent term. A Service Credit is added to the end of Client's current Subscription Term.
- May not be a financial refund or credit of any kind.
- Do not apply to failure of other service level SLAs if such failure relates to non-availability of the Service. In such cases Client may only submit a claim for the Availability SLA.

5.0 CLAIMS PROCESS

Client must submit the claim in writing via email to Coalfire Client Support at support@coalfire.com . Each claim must be submitted within ten (10) days of the end of the calendar month in which the alleged missed SLA occurred for Coalfire to review the claim. Each claim must include the following information:

1. The words "Service Credit Request" in the subject line.
2. The dates and time periods for each instance of claimed outage or other missed SLA, as applicable, during the relevant month.
3. An explanation of the claim made under this Service Description, including any relevant calculations.

All claims will be verified against Coalfire's system records. Should any claim be disputed, Coalfire will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide a record of service availability for the time period in question to Client.

6.0 EXCUSED OUTAGES AND EXCLUSIONS TO CLAIMS

The following are minutes of downtime that are defined as Excused Outages:

1. Planned Maintenance and Unplanned Maintenance as defined in the Service Description.
2. Force Majeure as defined in the Agreement.
3. Any downtime that results from any of the below listed exclusions to a claim.

If any of the following exclusions apply, a claim will not be accepted:

4. Any Service provided on a provisional basis, including but not limited to: trialware, evaluation, Proof of Concept, Not for Resale, pre-release, beta versions.
5. Client has not paid for the Service.
6. Third party, non-Coalfire branded products or services resold with the Service.
7. Hardware, software or other data center equipment or services not in the control of Coalfire or within the scope of the Service.
8. Technical support provided with the service.
9. Failure of Client to correctly configure the Service in accordance with this Service Description.
10. Hardware or software configuration changes made by the Client without the prior written consent of Coalfire.
11. Unavailability of a specific web page or a third party's cloud application(s).
12. Individual data center outage.
13. Unavailability of one or more specific features, functions, or equipment hosting locations within the service, while other key features remain available.
14. Failure of Client's Internet access connections.
15. Suspension and termination of Client's right to use the Service.
16. Alterations or modifications to the Service, unless altered or modified by Coalfire (or at the direction of or as approved by Coalfire
17. Defects in the Service due to abuse or use other than in accordance with Coalfire's published Documentation unless caused by Coalfire or its agents.
18. Client-requested hardware or software upgrades, moves, facility upgrades, etc.

END OF EXHIBIT A