Table of Contents

LevelBlue Threat Detection and Response for Government

LevelBlueThreat Detection and Response for Government ("the Service" or "TDR for Government") is a cloud-hosted security monitoring service. TDR for Government works to help detect and respond to advanced threats by combining multiple security technologies including asset discovery, vulnerability assessment, intrusion detection, endpoint detection and response, behavioral monitoring, SIEM log management, and continuous threat intelligence, powered by Alien LabsSM threat intelligence.

TDR for Government is available as a self-managed service or with 24/7 monitoring by LevelBlue's Security Operations Center.

The Service is designed to handle data that is subject to certain government regulations and requirements including, but not limited to, the following compliance standards:

- GSA FedRAMP for Cloud Service Providers
- National Institute of Standards and Technology (NIST) 800.171 standard
- NIST Security Content Automation Protocol (SCAP) v.1.3 Validation Program
- This Service Guide consists of the following parts:
- Service Description (SD)
- Service Level Objectives (SLO)
- Pricing (P)
- Country Specific Provisions (CSP)

In addition, specified portions of the General Provisions apply.

Service Description (SD)

SD-1. Operational Service Requirements

SD-1.1. Supported Environments for Sensor Deployment (Supported Environments)

Section Effective Date: 13-Apr-2021

- On Premises Data Centers (physical environments)
- VMWare®
- Hyper-V
- Infrastructure as a Service (IaaS) Public Cloud Environments
  - Amazon Web Services (AWS)
  - Microsoft Azure®
  - Google Cloud Platform™
- US Government-compliant Infrastructure as a Service (IaaS) Cloud Environments*
  - AWS GovCloud
  - Microsoft Azure® Government
  - Google Cloud Platform™

*Sensor restrictions apply to specific Supported Environments.

Cross References

SD-2.2.2. LevelBlue Threat Detection and Response for Government Sensors

SD-1.2. Customer Availability

Section Effective Date: 13-Apr-2021

At this time, the Service is only available to (a) U.S. federal, state, and local government entities; and (b) U.S. based companies with headquarters in the United States.

SD-1.3. Withdrawal of Service or Service Component

Section Effective Date: 31-Mar-2023

LevelBlue may discontinue providing Service upon 12 months' notice, or a Service Component upon 120 days' notice, but only where LevelBlue generally discontinues providing the Service or Service Component to similarly situated customers.

SD-2. TDR for Government – General Service

SD-2.1. Overview

Section Effective Date: 13-Apr-2021

The Service delivers near real-time log monitoring, event correlation, threat intelligence, and expert analysis of security activity across a Customer's entire enterprise. The Service receives a continuous stream of threat intelligence updates from both Alien Labs security research team and LevelBlue threat intelligence composed of third-party threat feeds and internal threat intelligence.

SD-2.1.1. FedRAMP Authorization

Section Effective Date: 13-Apr-2021

The Service is FedRAMP authorized at moderate level. It meets the U.S. government standards for cybersecurity requirements of cloud services in accordance with Federal Information Security Modernization Act (FISMA), the Office of Management and Budget (OMB) Circular A-130, and FedRAMP policy based on NIST standards and guidelines.

The Service has been awarded an Agency Authority to Operate (ATO) through FedRAMP federal agency authorization process. It is subject to FedRAMP governance framework.

SD-2.2. Service Component Minimum Requirements

Section Effective Date: 13-Apr-2021

One (1) LevelBlue Threat Detection and Response for Government Subscription

One (1) LevelBlue Threat Detection and Response for Government Sensor

SD-2.2.1. LevelBlue Threat Detection and Response for Government Subscription

SD-2.2.1.1. TDR for Government Subscription Editions

Section Effective Date: 13-Apr-2021

Actual features and capabilities of the Service depend on the LevelBlue Threat Detection and Response for Government Subscription Service Component (TDR for Government Subscription) purchased by Customer. The TDR for Government Subscription is sold in two different "Editions":

- Premium
- Premium 180

The Edition purchased by Customer is identified in the Service Agreement.

SD-2.2.1.1.1. TDR for Government Subscription Features

Section Effective Date: 13-Apr-2021

The following are features of each Edition:

	Edition	
Product Features	Premium	Premium 180
Asset Discovery and Inventory	Yes	Yes
Vulnerability Assessment	Yes	Yes
Intrusion Detection	Yes	Yes
Endpoint Detection and Response	Yes	Yes
Response Orchestration and Automation	Yes	Yes
Built-in Compliance Reports	Yes	Yes
Searchable Storage	90 days	180 days
Cold Storage	Yes	Yes
Threat Intelligence	Yes	Yes
User Accounts	Unlimited	Unlimited
Advanced AlienApps®	Yes	Yes
Advanced Security Notifications	Yes	Yes
Dark web monitoring	Yes	Yes

SD-2.2.1.1.1.1. Asset Discovery and Inventory

Section Effective Date: 13-Apr-2021

The Sensor performs Asset discovery in the Customer's environment via network scans, querying the hypervisor, cloud API, and active directory to identify connected assets, software, services, and configurations. Once discovered, Assets can be assigned to a group and device type. Assets can also be given a name, description, and compliance grouping. An "Asset" is an IP-addressable host, including but not limited to, network devices, virtual servers, and physical servers.

Cross References

[SD-2.2.2. LevelBlue Threat Detection and Response for Government Sensors]

SD-2.2.1.1.1.2. Vulnerability Assessment

Section Effective Date: 13-Apr-2021

Unauthenticated and authenticated scans can be performed on an ad hoc basis or scheduled based on Customer's preference. Vulnerability assessments are used for defining, identifying, classifying, and prioritizing the vulnerabilities in the Customer's system.

SD-2.2.1.1.1.3. Intrusion Detection

Section Effective Date: 13-Apr-2021

The Service delivers Host Intrusion Detection (HIDS), Network Intrusion Detection (NIDS), and cloud intrusion detection to detect anomalous or suspicious activities in a Customer's environment that may indicate an intrusion or attack.

SD-2.2.1.1.1.4. Endpoint Detection and Response (EDR)

Section Effective Date: 13-Apr-2021

The Service utilizes an AlienVault EDR agent (AlienVault Agent) to monitor the Customer's Assets activity, status, authentication, authorization, and software to detect and respond to advanced endpoint threats, including those designed to evade traditional antivirus tools. An installed AlienVault Agent communicates over an encrypted channel to send data directly to the Service.

SD-2.2.1.1.1.5. Response Orchestration and Automation

Section Effective Date: 13-Apr-2021

The Service utilizes orchestration and automation capabilities to help achieve faster incident response and to help improve the efficiency of the overall security team.

SD-2.2.1.1.1.6. Reporting

Section Effective Date: 13-Apr-2021

The Service has reporting functions that allow Customers to create reports based on details in the Customer's environment. Within the Service, the Customer has access to pre-built templates. These reports can be customized, saved, and exported by Customer as needed.

SD-2.2.1.1.1.7. Searchable Storage

Section Effective Date: 13-Apr-2021

During the Service Term, Customers can access Events, Alarms, and vulnerabilities from the previous 90, or 180 days (depending on the purchased Edition) within the Service.

SD-2.2.1.1.1.8. Cold Storage

Section Effective Date: 13-Apr-2021

During the Service Term, Customer's raw log data is stored in cold storage. Customer may request a raw log data file in raw format from cold storage at any time through the Service dashboard during the Service Term.

SD-2.2.1.1.1.9. Threat Intelligence

Section Effective Date: 13-Apr-2021

The Service analyzes Events and Customer Data against the latest correlation rules within TDR for Government. Correlation rules are added and updated on a regular basis by the Alien Labs security research team, who utilize security data from the Open Threat Exchange® (OTX), third party threat feeds, and internal threat intelligence.

SD-2.2.1.1.1.10. User Accounts

Section Effective Date: 13-Apr-2021

The Service provides Customer with the ability to manage (add, modify, and delete) User accounts.

SD-2.2.1.1.1.11. BlueApps® and Advanced BlueApps

Section Effective Date: 13-Apr-2021

BlueApps extend the capabilities of the Service through integrations with leading third-party security tools, providing a consolidated approach to threat detection. BlueApps are included in all Editions. As a part of the Service, Customers also receive "Advanced BlueApps" which include the following additional features:

- an added orchestration ability that enables Customers to automate response actions with the Customer's on-premises and cloud infrastructure as well as third-party security applications, and
- additional BlueApp availability including specific BlueApp dashboards.

SD-2.2.1.1.1.12. Security Notification

Section Effective Date: 13-Apr-2021

In the event of a critical security alert, the Service can automatically send email notification to the Customer. As a part of the Service, these alerts can also be automated with certain third-party software or services (Advanced Security Notification) so Customers can receive notifications through those third-party interfaces.

SD-2.2.1.1.1.13. Dark Web Monitoring

Section Effective Date: 13-Apr-2021

The Service can alert Customer of stolen user credentials discovered on the dark web. This type of watchlist feature is limited to 1 domain and up to 10 email addresses.

SD-2.2.1.1.1.14. Supports PCI Log Storage Requirement

Section Effective Date: 13-Apr-2021

The Service supports Payment Card Industry Data Security Standards (PCI DSS) log retention policies.

SD-2.2.1.1.1.15. Supports FIPS 140-2 Encryption

Section Effective Date: 13-Apr-2021

The Service supports the NIST Federal Information Processing Standards (FIPS) publication 140-2 (FIPS 140-2). FIPS 140-2 is a U.S. government computer security standard used to approve cryptographic modules.

SD-2.2.1.1.2. Limitations of the Subscriptions

Section Effective Date: 13-Apr-2021

Each TDR for Government Subscription has a monthly usage limit. Customer's usage limit is the numeric value specified in the name of the TDR for Government Subscription purchased by Customer in the Service Agreement (Usage Limit).

SD-2.2.1.1.2.1. Usage Limit Purchase Options

Section Effective Date: 13-Apr-2021

TDR for Government Subscriptions are available with Usage Limits between 250GB and 60TB.

SD-2.2.2. LevelBlue Threat Detection and Response for Government Sensors

Section Effective Date: 31-Mar-2023

LevelBlue Threat Detection and Response for Government Sensors (Sensors) are virtualized software that Customer can deploy into Customer's Supported Environments and link to a TDR for Government Subscription to collect log and other security-related data. This data is normalized and then forwarded to TDR for Government, hosted in AWS, for analysis and correlation.

Customer will be provided with a list of available sensors (Standard and Gov) and may download and deploy whichever is appropriate for their environment(s).

Cross References

SD-1.1. Supported Environments for Sensor Deployment (Supported Environments)

SD-2.8. Deployment of Sensor

SD-2.3. Optional Add-On Service Components

Section Effective Date: 31-Mar-2023

Customers may purchase optional additional Service Components listed below. Individual requirements may apply based upon the Service Component.

- LevelBlue Threat Detection and Response for Government, Implementation Services
- LevelBlue Threat Detection and Response for Government Training, USM Anywhere Training Pass
- LiftOff Package
- LevelBlue Threat Detection and Response for Government, Remote Consultant

- 24/7 managed security monitoring services by LevelBlue Security Operations Center (SOC) (LevelBlue Managed Threat Detection and Response for Government).

SD-2.3.1. LevelBlue Threat Detection and Response for Government, Implementation Services

Section Effective Date: 13-Apr-2021

Implementation Services assist Customers with the initial deployment and configuration of the Service so the Service can begin to detect threats (Implementation Services).

When purchased as an add-on Service Component, Customer receives four (4) hours of assistance with an Implementation Services consultant. Implementation Services are delivered remotely.

Implementation Services may also be purchased as part of the LiftOff Package.

Cross References

SD-2.3.1.1. Scope of Implementation Services

Section Effective Date: 13-Apr-2021

During the Implementation Services consultation, Customers will participate in an initial orientation and planning call (Kick-Off Call) during which time the scope will be defined. The following tasks are available as a part of the Implementation Services:

- Deploying Sensors
- Enabling Asset discovery
- Configuring and scheduling and initial vulnerability scan
- Configuring log forwarding (Asset to Sensor)
- Configuring Asset credentials
- Configuring static and dynamic Asset groups
- Configuring orchestration rules
- Creating custom reports
- Configuring Advanced BlueApps
- Configuring Security Notification methods

- Linking an OTX™ account
- Creating custom Event views

SD-2.3.1.2. Commencement of Implementation Services and the Engagement

Section Effective Date: 13-Apr-2021

Customer will receive an Onboarding Email and will be assigned to an Implementation Services consultant. Customer and the consultant will schedule a date and time for the Implementation Services Kick-off Call.

SD-2.3.1.3. Implementation Service Restrictions and Requirements

Section Effective Date: 13-Apr-2021

- To purchase Implementation Services, Customer must have, or be purchasing concurrently, a minimum of one (1) active TDR for Government Subscription and one (1) active Sensor.
- Implementation Services must be used before the expiration of 180 calendar days following the date of the Onboarding Email for the purchased Implementation Services. If Implementation Services are not utilized within this time frame, Customer will forfeit any remaining hours and will not be entitled to receive any credits or refund for any unused hours.
- Implementation Services are available in English only.

SD-2.3.2. LevelBlue Threat Detection and Response for Government Training, USM Anywhere Training Pass

Training courses provide Customers with expert instruction and hands-on product training to help deploy, manage, and use the Service. Training is delivered live online by certified instructors.

When the LevelBlue Threat Detection and Response for Government Training, USM Anywhere Training Pass is purchased as an add-on Service Component, Customer receives:

- One (1) Delegate Pass that may be redeemed for one (1) of the two (2) training courses listed in this Service Guide, and
- One (1) AlienVault Security Engineer (AVSE) exam voucher.

Training may also be purchased as part of the LiftOff Package.

Cross References

SD-2.3.3. LiftOff Package

SD-2.3.2.1. Training Courses

Section Effective Date: 13-Apr-2021

Customer may redeem a Delegate Pass for one of two (2) available Training courses:

- USM Anywhere: Deploy, Configure, Manage (ANYDC)
- This two-day course prepares Customers to implement and operate the Service.
- USM Anywhere: Security Analysis (ANYSA)

This two-day course provides Customer security analysts with the knowledge and tools to utilize the Service to assist with analyst duties.

SD-2.3.2.1.1. AlienVault USM Certified Security Engineer Certification

Section Effective Date: 13-Apr-2021

The AVSE validates the Customer's knowledge and skills of the Service.

Upon completion of a training course, Customer will receive an email from LevelBlue with their AVSE exam voucher number, confirmation of the AVSE exam voucher expiration date, and complete instructions on how to register for the AVSE exam. The exam voucher is redeemable for the AVSE certification exam.

SD-2.3.2.2. Training Requirements and Restrictions

Section Effective Date: 13-Apr-2021

- The Delegate Pass expires 180 calendar days from the date of the Onboarding Email. If the Delegate Pass is not used within 180 calendar days following the Onboarding Email, Customer will not be entitled to receive any credits or refund for any unused Training.
- The AVSE voucher expires 180 calendar days from the date the AVSE voucher is sent via email to Customer, which expiration date will be confirmed in the email sent to Customer. The AVSE exam must be taken on or before the voucher expiration date. The AVSE exam voucher can only be used once.

- If Customer does not complete a training course, Customer will forfeit the associated AVSE voucher.

- Training is available in English only.

SD-2.3.3. LiftOff Package

Section Effective Date: 13-Apr-2021

A LiftOff Package is designed to help Customers get the Service up and running quickly. Each "LiftOff Package" includes two Service Components but they are listed separately on the Service Agreement, as noted below.

- LevelBlue Threat Detection and Response for Government, Implementation Services
- LevelBlue Threat Detection and Response for Government Training, USM Anywhere Training Pass

SD-2.3.3.1. LiftOff Package, Implementation Services

Section Effective Date: 13-Apr-2021

Implementation Services assist Customers with the initial deployment and configuration of the Service so the Service can begin to detect threats.

The number of hours included in the LiftOff Package Implementation Services are based on the Usage Limit of Customer's purchased TDR for Government Subscription as outlined in the table below.

LiftOff Package, Implementation Services	
Usage Limit	**Implementation Service**
250GB – 1TB	4
1.5TB – 2TB	8
3TB – 4TB	12
6TB	16
8TB – 20TB	32
40TB – 60TB	40

All Implementation Services are delivered by a consultant remotely.

SD-2.3.3.1.1. Scope of Implementation Services for LiftOff Package

Section Effective Date: 13-Apr-2021

During the Implementation Services consultation, Customers will participate in an initial orientation and planning call (Kick-Off Call) during which time the scope will be defined. The following tasks are available as a part of the Implementation Services:

- Deploying Sensors
- Enabling Asset discovery
- Configuring and scheduling an initial vulnerability scan
- Configuring log forwarding (Asset to Sensor)
- Configuring Asset credentials
- Configuring static and dynamic Asset groups
- Configuring orchestration rules
- Creating custom reports
- Configuring Advanced BlueApps
- Configuring Security Notification methods
- Linking an OTX™ account
- Creating custom Event views

SD-2.3.3.2. LiftOff Package, Training

Section Effective Date: 13-Apr-2021

Training provides Customers with expert instruction and hands-on product training to help deploy, manage, and use the Service. This training is delivered live online by certified instructors.

The number of Delegate Passes and AVSE Vouchers is based on the Usage Limit of Customer's purchased TDR for Government Subscription.

LiftOff Package, Training		
Usage Limit	**Delegate Passes**	**AVSE Vouchers**
250GB – 1TB	2	2
1.5TB – 2TB	3	3

SD-2.3.3.2.1. Training Courses

Section Effective Date: 13-Apr-2021

The Training Courses listed in this Service Guide are available to Customers purchasing the LiftOff Package.

Cross References

SD-2.3.2.1. Training Courses

SD-2.3.3.2.1.1. AlienVault USM Certified Security Engineer Certification

Section Effective Date: 13-Apr-2021

AlienVault USM Certified Security Engineer Certification described in this Service Guide is also available to Customers purchasing the LiftOff Package.

Cross References

SD-2.3.2.1.1. AlienVault USM Certified Security Engineer Certification

SD-2.3.3.3. LiftOff Package Commencement

Section Effective Date: 13-Apr-2021

An Onboarding Email will be sent to the Customer confirming the LiftOff Package purchase.

- Implementation Services: Following the Onboarding Email, Customer will be assigned to an Implementation Services consultant and receive an email of introduction. Customer and the consultant will schedule a date and time for the Kick-Off Call.
- Training:
  - Following the Onboarding Email, Customer will receive a second email with a voucher number for each Delegate Pass and instructions detailing how to sign up for a training course.

- Upon completion of a training course, Customer will receive an email from LevelBlue with their AVSE exam voucher number, confirmation of the AVSE exam voucher expiration date, and complete instructions on how to register for the AVSE exam.

SD-2.3.3.4. LiftOff Package Requirements and Restrictions

Section Effective Date: 13-Apr-2021

- Any Service Components identified as "LiftOff Package" can only be purchased as a part of the package at the time of the initial TDR for Government Subscription purchase. Components without the "LiftOff Package" designation can be sold individually.
- Customer can only purchase a LiftOff Package that corresponds with their current TDR for Government Subscription Edition and/or Usage Limit.
- With the exception of the AVSE voucher, the LiftOff Package expires 180 calendar days, from the date of the Onboarding Email. If the LiftOff Package is not used, in whole or in part, within 180 calendar days following the Onboarding Email, Customer will not be entitled to receive any credits or refund for any unused portion of the LiftOff Package.
- The AVSE voucher expires 180 calendar days from the date the AVSE voucher is sent via email to Customer, which expiration date will be confirmed in the email sent to Customer. The AVSE exam must be taken on or before the voucher expiration date. The AVSE voucher can only be used once.
    - If Customer does not complete a training course, Customer will forfeit the associated AVSE voucher.
- LiftOff Package is available in English only.

SD-2.3.4. TDR for Government, Remote Consultant

Section Effective Date: 13-Apr-2021

TDR for Government Remote Consultant services can be purchased to assist Customers with additional configuration and management of the Service after the Customer's initial deployment and configuration of the Service (Remote Consultant Services).

Customer receives 8 hours of remote assistance with a purchase of Remote Consultant Services.

SD-2.3.4.1. Scope of Remote Consultant

Section Effective Date: 13-Apr-2021

During the Remote Consultant Services, Customers may request assistance with any of the following tasks, which will be agreed upon before the commencement of the tasks:

- Deploying additional Sensors
- Enabling Asset discovery
- Configuring and scheduling vulnerability scans
- Configuring log forwarding (Asset to Sensor)
- Configuring Asset credentials
- Configuring static and dynamic Asset groups
- Configuring orchestration rules
- Creating custom reports
- Configuring Advanced AlienApps
- Configuring Security Notification methods
- Creating custom Event views
- Configuring NIDS and AWS IDS
- Rsyslog / syslog-ng configurations
- NXlog customizations
- Troubleshooting and problem resolution

SD-2.3.4.2. Commencement of Remote Consultant Services and the Engagement

Section Effective Date: 13-Apr-2021

Following an Onboarding Email, Customer will be assigned to a consultant and receive an email of introduction. Customer and the consultant will schedule a date and time for the Remote Consultant Services.

SD-2.3.4.3. Remote Consultant Restrictions and Requirements

Section Effective Date: 31-Mar-2023

- To purchase the Remote Consultant Services, Customer must have, or be purchasing concurrently, a minimum of one (1) active TDR for Government Subscription and one (1) active Sensor.
- Remote Consultant Services must be used before the expiration of 180 calendar days following the date of the Onboarding Email for the purchased Remote Consultant Services; otherwise, Customer will forfeit any remaining hours and will not be entitled to receive any credits or refund for any unused hours.
- Remote Consultant Services are available in English only.

SD-2.3.5. Managed Threat Detection and Response for Government

SD-2.3.5.1. Description

Section Effective Date: 31-Mar-2023

Managed Threat Detection and Response for Government (MTDR for Government) is Service Component of Threat Detection and Response for Government that provides a centralized managed security monitoring service that delivers near real-time event monitoring, rule correlation, vulnerability assessment, external indicators of compromise (IoC) matching, asset discovery and inventory, and expert analysis of security incidents across an enterprise 24/7. The MTDR for Government is designed to identify cybersecurity risks to the organization and helps improve cybersecurity posture through investigation management across on-premises, cloud, and hybrid IT environments.

Available features are the same as TDR for Government with the following exceptions:

- The Service Activation Date will be thirty (30) calendar days from the time Customer's Subscription is issued. LevelBlue will contact Customer for a formal kick-off call to discuss service delivery.
- Platform Access – Customers have 24/7 access to all the functionalities within the TDR for Government Service using two-factor authentication.
- MTDR for Government Subscriptions are available with Usage Limits between 500GB and 60TB.
- The table below reflects the maximum sensors included per Tier purchased in the Service Agreement. Additional sensors can be purchased per Tier and will incur additional monthly recurring charges.

LevelBlue Managed Threat Detection and Response for Government	
Service	**Max Sensors per Tier**
Maximum Subscription Tier	
LevelBlue Managed Threat Detection and Response for Government (500GB)	9
LevelBlue Managed Threat Detection and Response for Government (1TB)	9
LevelBlue Managed Threat Detection and Response for Government (1.5TB)	9
LevelBlue Managed Threat Detection and Response for Government (2TB)	9
LevelBlue Managed Threat Detection and Response for Government (3TB)	18
LevelBlue Managed Threat Detection and Response for Government (4TB)	18
LevelBlue Managed Threat Detection and Response for Government (6TB)	18
LevelBlue Managed Threat Detection and Response for Government (8TB)	18
LevelBlue Managed Threat Detection and Response for Government (10TB)	36
LevelBlue Managed Threat Detection and Response for Government (15TB)	36
LevelBlue Managed Threat Detection and Response for Government (20TB)	36
LevelBlue Managed Threat Detection and Response for Government (25TB)	36
LevelBlue Managed Threat Detection and Response for Government (30TB)	36
LevelBlue Managed Threat Detection and Response for Government (40TB)	72
LevelBlue Managed Threat Detection and Response for Government (50TB)	72
LevelBlue Managed Threat Detection and Response for Government (60TB)	72

Implementation Services are not available as an additional Service Component with Managed Threat Detection and Response for Government

SD-2.3.5.2. Customer Engagement Plan

Section Effective Date: 31-Mar-2023

The Customer Engagement Plan (CEP) establishes an agreed framework for responding to identified security incidents. The CEP establishes procedures for validating, categorizing, documenting, and communicating security events identified by the Service.

LevelBlue does not guarantee that remediation steps taken in accordance with the CEP will be effective against threats, attacks and unauthorized intrusions on Customer's network environment. Customer is solely responsible for any adverse consequences on its network environment resulting from remediation steps taken in accordance with the CEP. LevelBlue is not liable for damages or costs that may be caused by the implementation of the CEP.

SD-2.3.5.3. Availability

Section Effective Date: 31-Mar-2023

Customer support for security related issues will be available 24/7 through the LevelBlue SOC.

SD-2.3.5.4. Service Onboarding

Section Effective Date: 31-Mar-2023

To ensure a successful Service Onboarding, Customer is responsible for the following:

- Provide a technical contact who will participate in delivery of service
- Attend regularly scheduled meetings with action items completed
- Provide a list of all users needing access to the platforms

SD-2.3.5.5. Support Availability

Section Effective Date: 31-Mar-2023

Support for MTDR for Government is provided by US Citizens located in the 48 contiguous United States and the District of Columbia.

- Customer support for security incidents will be available 24/7 through the LevelBlue SOC. Customers can reach the SOC utilizing three different forms of contact.

- Call: 1-844-359-7055
- Email: MTDR-Gov@att.com
- Submit an Investigation on the USM Platform

The Service will process all Events, Alarms, and Investigations pertaining to the Service and will post this information on the USM Platform.

- If technical support for low severity non-security incidents requires referral to USM Escalation team, hours are 8:00am to 6:00pm Eastern Time (ET), Monday through Friday, excluding the holidays identified in the General Provisions. The following types of assistance are available to Customers during the applicable support hours:
  - Technical Support: Identifying, analyzing, and resolving challenges preventing the Service from operating as it was designed
  - Data Storage and Retention: Retention of Customer Data stored within the Service, as described in this Service Guide, during the applicable Service Term.

When a designated holiday falls on a Saturday or Sunday, the date observed for that designated holiday may be either the previous Friday or subsequent Monday.

SD-2.3.5.6. Supported Device List

Section Effective Date: 31-Mar-2023

During onboarding for MTDR for Government, only the device types, device quantities and data collection site locations previously reviewed and approved by LevelBlue will be included within the scope for onboarding. Any changes to the device types, device quantities or data collection site locations will require additional review and approval by LevelBlue. If the scope of onboarding leads to a change in commitment level, Customer will be responsible for any adjustments to pricing. Customer changes to the list of monitored devices must be provided in writing to LevelBlue within ten business day prior to such change(s) taking effect.

SD-2.3.5.7. Customer Responsibilities

Section Effective Date: 31-Mar-2023

To qualify for MTDR for Government, Customer is responsible for:

- Assigning a Single Point of Contact (SPOC).

- Providing network and security documentation and information necessary to all LevelBlue resources involved with MTDR for Government to assess and review the network being monitored.
- Providing the initial list of Customer-defined devices in writing to LevelBlue prior to onboarding.
- Providing LevelBlue-specified technical device information for each Customer-defined device.
- Providing secure network transport and associated hardware, if applicable, to transmit information from the LevelBlue-provided data collector(s) to MTDR for Government.

SD-2.4. Monthly Storage Usage Limit

Section Effective Date: 13-Apr-2021

The Service has usage limitations. Customer's monthly Usage Limit is the numeric value specified in the Pricing Schedule ("Usage Limit"). Monthly storage Usage Limits will be monitored and tracked by LevelBlue. Customer will, at all times, ensure that its use of the Service does not exceed the Usage Limit.

Where a Customer's usage of the Service exceeds the Usage Limit, its Service will be impacted as set forth below:

- Caution Mode – The USM Platform will (i) display an early and persistent warning to inform Customer that their monthly tiered usage is going to be exceeded, and (ii) in the event that Customer exceeds their Usage Limit, the subscription will enter Caution Mode and the environment will display a notification indicating so.
- Warning Mode – An environment in Warning Mode will operate normally, except that no new sensors or integrations can be set up or configured while in this mode.
- Violation Mode – Subscriptions in Violation Mode no longer store Events in the searchable data store, but will still generate Alarms, run Authenticated Asset Scans, and store Raw Logs associated with Events in Cold Storage. In this mode, searches are limited to the most recent 24 hours for Events, Alarms, and vulnerabilities.
- Recovery Mode – While the environment is in Caution, Warning, or Violation Mode, Customers can request to enter Recovery Mode. If the projected monthly data consumption reassessment is under the threshold for the subscription tier, the environment will transition to Recovery Mode. If the projected data consumption is still above the tier threshold after the 24-hour reassessment, the environment will

transition out of Recovery Mode and into the mode appropriate to the new projected data consumption. Please note that Recovery Mode can only be requested up to three times a month.

If Customer continues to exceed the Usage Limit, LevelBlue will have the right, in its discretion, to immediately suspend Customer's use of the Service and, with no less than 30 days' notice, terminate the Service. Customer acknowledges that its use of the Service in excess of Usage Limit may result in a significant degradation in the performance. Any suspension or termination of the Service under this section will not relieve Customer of its payment obligations associated with the Service.

SD-2.5. Subdomain Key

Section Effective Date: 31-Mar-2023

The TDR for Government Subscription is assigned a unique subdomain name (Subdomain Key). The Subdomain Key may be requested and will be set forth on the Service Agreement. Customer acknowledges that LevelBlue cannot commit that a requested Subdomain will be assigned to the purchased Service Component. A requested Subdomain may be unavailable at the time that LevelBlue provides Service Activation. In that event, LevelBlue will assign a substantially similar Subdomain as determined by LevelBlue.

Sensors are mapped to a TDR for Government Subscription by assigning them the same Subdomain of the TDR for Government Subscription.

SD-2.6. Change Control Process

Section Effective Date: 13-Apr-2021

To purchase an additional Service Component, upgrade a Service Component, or renew a Service Component during the Service Term, Customer must contact its LevelBlue sales representative. Any changes will be effective upon execution of an additional Service Agreement.

SD-2.7. Use of Service

Section Effective Date: 13-Apr-2021

Subject to the limitations stated in this Service Guide, Customer is granted a limited, non-exclusive, revocable, non-transferable, non-sublicensable right during the applicable Service Term to use the Service, Documentation, and LevelBlue Software in accordance with the scope of use specified in this Service Guide.

SD-2.7.1. User Account Credentials

Section Effective Date: 13-Apr-2021

Customer is responsible for maintaining the confidentiality of the administrator and User logon identifications, passwords, and account information.

SD-2.7.2. Compliance and Use

Section Effective Date: 13-Apr-2021

Customer will be responsible for Users' compliance with this Service Guide. Customer will use the Service in accordance with the Documentation, the Acceptable Use Policy, and all applicable laws and government regulations.

Customer will use commercially reasonable efforts to prevent unauthorized access to or use of the Service and all Documentation. If there is unauthorized access or use of the Service or Documentation by anyone who obtained access to the Service or Documentation directly or indirectly through Customer, Customer will take all steps reasonably necessary to terminate the unauthorized use, and must immediately notify LevelBlue. Customer will cooperate and assist with any actions taken by LevelBlue to prevent or terminate unauthorized use of the Service or any Documentation.

SD-2.7.3. Limitations and Restrictions on Use of the Service

Section Effective Date: 13-Apr-2021

Customer will comply with the following limitations and restrictions when using the Service:

- Except as otherwise expressly approved by LevelBlue in writing or as is required by applicable law, Customer will not, and will not permit or authorize Users to:
  - attempt to modify, create derivative works from, frame, mirror, republish, download, display, transmit, distribute, reverse compile, disassemble, reverse engineer, or otherwise reduce to human-perceivable form all or any portion of the Service, or LevelBlue Software in any form or media or by any means;
  - access all or any part of the Service, Documentation, or LevelBlue Software in order to build a product or service that competes with the Services;
  - license, sell, rent, lease, transfer, assign, distribute, display, disclose, or otherwise commercially exploit the Service, Documentation, or LevelBlue

Software, or otherwise allow it to be available to any third party (e.g., as a hosted service or service bureau);

- circumvent or disable (or attempt to circumvent or disable) any protection, restriction, security, or other technological features or measures of the Service, Documentation, or LevelBlue Software;
- perform unauthorized probes or scans with the intent to gather information on possible weaknesses or exploitable configurations;
- use the Service, Documentation, or LevelBlue Software for any purpose other than Customer's internal business purposes in relation to its own computer-related systems and any computer-related systems or facilities owned or managed exclusively by or for Customer;
- develop any type of software program based on the Service, Documentation, or LevelBlue Software;
- provide or offer access to any third parties to any restricted online access keys or authentication passwords provided by LevelBlue; or
- disclose to any third party any benchmarking or comparative study involving the Service.

- Compatibility with Third-Party Software. Customer consents and acknowledges that prior to upgrading or adding third-party software, the Customer is solely responsible to verify and ensure that such third-party software is compatible with their current or future versions of the Service. LevelBlue will not be responsible for any failures or malfunctions' resulting from such upgrade, change, or addition of third-party software and will not provide support for such installations.
- Input/Output of Data and Lost Files. Customer is solely responsible for the placement of Sensors and AlienVault Agents in their environment to allow for visibility of its data input and output to the Service and for maintaining a separate means for the reconstruction of any lost data.
- Accuracy Disclaimer. Customer is solely responsible for the accuracy and integrity of its own data, reports, and documentation. LevelBlue may provide links to other websites or resources as part of the Service or Documentation. LevelBlue does not endorse and is not responsible for any data, software, or other content available from such websites or resources. Customer acknowledges and agrees that LevelBlue will not be liable, directly or indirectly, for any damage or loss relating to Customer's use of or reliance on such data, software, or other content.

- Customer is responsible for purchasing and maintaining its own equipment, hardware, and access, including but not limited to network and data connection, to establish a connection to the Internet.
- Application Program Interfaces (APIs). APIs, provided as a part of the Service, are provided "as is" without any warranty whatsoever. Customer is granted a personal, non-sublicensable, nonexclusive, nontransferable, limited license to use the API solely for Customer's internal use for exporting Customer's content from LevelBlue to the new Customer system. Customer may not (a) copy, rent, sell, disassemble, reverse engineer or decompile (except to the limited extent expressly authorized by applicable statutory law), modify or alter any part of the API; or (b) otherwise use the API on behalf of any third party. The API license shall automatically terminate in the event Customer breaches this section.
- Data Limitations. Ingestion of data does not necessarily imply that an existing correlation rule will be present to initiate an alarm for an Analyst to triage. We are not required to create Alarms from every data source nor does the Managed SOC team provide coverage of all data types.

SD-2.8. Deployment of Sensor

Section Effective Date: 31-Mar-2023

Customer agrees to follow LevelBlue's detailed installation steps for deployment of sensor software across the Customer's Cloud or Virtual Environments, as the case may be, and that LevelBlue will be given remote access to the sensors for the Service, including for the purposes of ascertaining system performance and accessing system logs. Customer agrees that LevelBlue may disclose to third parties descriptions of security-related activities encountered by Threat Detection and Response for Government in Customer's environment, provided that such descriptions maintain the anonymity of Customer or Users.

SD-2.9. Audit

Section Effective Date: 13-Apr-2021

Customer will permit LevelBlue to audit use of the Service by Customer and Users. Such audit may be conducted no more than once per twelve months, at LevelBlue's expense, and this right will be exercised with reasonable prior notice, in such a manner as not to interfere with Customer's normal conduct of business. If the audit finds that Customer has underpaid any Service fees to LevelBlue, Customer will pay to LevelBlue an amount equal to such underpayment within 30 days of receipt of notice of such underpayment.

SD-2.10. Customer Data

Section Effective Date: 13-Apr-2021

Customer and its Users control the data, including volume and type, sent through the Service for analysis and storage from Customer's environment (Customer Data). Customer will retain all of its rights, title, and interest in and to Customer Data associated with the Service and all of its intellectual property rights including copyright, trademark, and trade secret rights in Customer Data. Customer hereby grants to LevelBlue (including Affiliates and subcontractors), throughout the Service Term and after the Service Term as necessary for any of LevelBlue's post-termination obligations to Customer, the necessary rights or license to use Customer Data as necessary to perform obligations related to the Service. Customer will not provide to LevelBlue, or store as part of its use of the Service, Customer Data that includes Payment Card Industry (PCI) data or Protected Health Information (PHI) data. Customer will provide LevelBlue in the form and format and on the schedule specified by LevelBlue, Customer Data as is reasonably required for LevelBlue's performance of the Service. Customer grants to LevelBlue (including Affiliates and subcontractors) a sublicensable and royalty free license to use such Customer Data in order to provide the Service to Customer and the Users and as necessary to access the Service to monitor and diagnose issues related to the Service. Customer is responsible for maintaining back-up on all Customer Data. Customer is responsible for the accuracy, quality, integrity, and legality of Customer Data and of the means by which Customer acquired Customer Data. Following expiration of the Service Term, Customer Data will be unless legally prohibited. This deletion may occur at any time during the thirty (30) calendar days following expiration of the Service Term.

SD-2.11. Product Usage Data

Section Effective Date: 31-Mar-2023

Customer agrees that LevelBlue may use information about how Customer uses the Service to generate statistics and to otherwise compile, synthesize and analyze such information for the purpose of operating, maintaining, repairing and improving the Service (Product Usage Data). Product Usage Data does not include Customer Data.

SD-2.12. Privacy Policy

Section Effective Date: 31-Mar-2023

Information obtained through the Service is governed by the Privacy Policy located at https://cybersecurity.att.com/legal/privacy-policy.

SD-2.13. Intellectual Property Rights

Section Effective Date: 13-Apr-2021

- All intellectual property and proprietary rights arising by virtue of LevelBlue's performance of the Services are and will be the sole and exclusive property of LevelBlue, and neither ownership nor title to any such property will pass to Customer.
- Customer will own copies of any Customer Reports. Customer is hereby granted, under LevelBlue's copyrights, the non-exclusive, personal, and non-transferable right to reproduce and modify Customer Reports for Customer's own internal business purposes. For avoidance of doubt, "internal business purposes" exclude public distribution, resale to third parties, and revenue generation purposes.
- LevelBlue will own all right, title, and interest in and to all modifications or derivatives of, and improvements to, the Service and all Documentation and any other part of the Services (created by either party). Customer hereby makes all assignments necessary to provide LevelBlue the ownership rights set forth in the preceding sentence.
- Except as otherwise expressly specified in this Service Guide, no other right or license to or under any of LevelBlue's intellectual property rights is either granted or implied hereunder.

SD-2.14. Compliance with Laws

Section Effective Date: 13-Apr-2021

LevelBlue provides this Service for a cybersecurity purpose, and in the U.S, both Customer and LevelBlue agree to comply with the Cybersecurity Information Sharing Act of 2015 (CISA). When using the Service, Customer agrees to monitoring by LevelBlue and designs and sets all filtering and interception policies (Security Policies). LevelBlue undertakes only to implement the Security Policies as directed by Customer and accepts no responsibility for the design or appropriateness of such design or settings. As between LevelBlue and Customer, when using the Service, Customer is solely responsible for obtaining and complying with the authorizations, licenses, and permissions required by law or by its suppliers or providers to enable the Service to access data on Customer's applications or products. Customer is responsible for obtaining consent from and giving notice to its Users regarding Customer's and LevelBlue's collection and use of User information in connection with the Service and regarding interception and/or monitoring of communications, including email and Internet use, associated with the Security Policies and the Service. Customer is

responsible for obtaining agreement from its Users to provide reasonable cooperation with LevelBlue in connection with responses to requests or requirements regarding the Service by any regulator, authority and/or other governmental entity.

SD-2.15. Service Support and Maintenance

Section Effective Date: 13-Apr-2021

Support for the Service is provided by US Citizens located in the 48 contiguous United States and the District of Columbia.

SD-2.15.1. Support Availability

SD-2.15.1.1. Primary Support Hours

Section Effective Date: 13-Apr-2021

Primary Support Hours are 8:00am to 6:00pm Eastern Time (ET), Monday through Friday, excluding the holidays identified in the General Provisions.

When a designated holiday falls on a Saturday or Sunday, the date observed for that designated holiday may be either the previous Friday or subsequent Monday.

SD-2.15.2. Support Scope

Section Effective Date: 13-Apr-2021

The following types of assistance are available to Customers during the applicable Support Hours:

- Technical Support: Identifying, analyzing, and resolving challenges preventing the Service from operating as it was designed
- Service Management: Client activation, change control, problem management, escalation procedures, and security monitoring and incident response of infrastructure operated and managed by LevelBlue
- Service Administration: Installation and server setup, support, response, repair, and operational monitoring and incident response of infrastructure operated and managed by LevelBlue
- Data Storage and Retention: Retention of Customer Data stored within the Service, as described in this Service Guide, during the applicable Service Term.

SD-2.15.2.1. Scope of Support Exclusions

Section Effective Date: 13-Apr-2021

- Maintenance and support for non-production environments and sand boxes
- Data migration
- Training
- Installation, configuration, and technical support for Customer equipment or operating systems
- Technical support, consultation, or problem resolution pertaining to software or applications other than those supplied by LevelBlue and described in this Service Agreement
- Resolution of problems resulting from negligence of users of the Service, including specifically incorrect data entry, use of altered data, and failure to use the Service according to the Documentation
- Support for development (AlienVault SDK, Web pages, etc.), integration and custom reports, whether developed by Customer or any party other than LevelBlue
- Any alterations or additions, performed by parties other than LevelBlue
- Use of the Service on an operating environment other than that for which such the Service was designed.

SD-2.15.3. Maintenance

Section Effective Date: 13-Apr-2021

LevelBlue periodically adds, repairs, and upgrades the data center network, hardware, and the Service and will use commercially reasonable efforts to accomplish this without affecting the Customer's access to the Service; however, repairs of an emergency or critical nature may result in the Service not being available for the Customer's usage during the course of such repairs. LevelBlue reserves the right to take down the server(s) at the data center in order to conduct routine maintenance to both LevelBlue Software and hardware according to the following protocols:

- "Maintenance" time can be either for "Scheduled Maintenance", "Preventative Maintenance", or "Emergency Maintenance".

- "Scheduled Maintenance" is routine, scheduled maintenance performed weekly on one of Tuesday, Wednesday, or Thursday between the hours of 12am and 4am PST (Maintenance Window). A message will be displayed on the product status page located at http://status.alienvault.cloud/ (Product Status Page) stating the Service will be unavailable. LevelBlue reserves the right to modify the Maintenance Window; provided, however, LevelBlue will provide notice to the Customer of such modification.
- "Preventative Maintenance" is non-scheduled scheduled maintenance that needs to be promptly conducted. LevelBlue will use commercially reasonable efforts to notify Customer by displaying a message on the Product Status Page before performing such Preventative Maintenance.
- "Emergency Maintenance" is unscheduled maintenance, repair or updating activities that are required to be performed immediately in order to protect LevelBlue facilities, network services or the security of Customer equipment or property. LevelBlue will attempt to provide reasonable notice to the Customer by posting notice on the Product Status Page when LevelBlue determines that it is required to perform Emergency Maintenance. Customer understands that Emergency Maintenance may be performed with little or no advance notice.

SD-2.15.4. Customer Support Responsibilities

SD-2.15.4.1. Primary Technical Contacts

Section Effective Date: 13-Apr-2021

Customer will designate at least two (2) individuals within Customer's organization to serve as primary contact with regards to support for Customer's Service (Primary Technical Contact). Primary Technical Contact should have sufficient technical knowledge of Customer's environment to enable effective communication with LevelBlue representatives.

SD-2.15.4.2. Customer Cooperation

Section Effective Date: 13-Apr-2021

Customer will provide LevelBlue with (i) reasonable access to all necessary personnel to answer questions regarding Issues reported by Customer, (ii) all relevant and available diagnostic information (including product or system information), and (iii) appropriate remote access to Customer's system to assist LevelBlue in isolating the cause and to resolve the Issue. In addition, Customer will make reasonable efforts to

correct any Issue, deploy corrections after consulting with LevelBlue, and promptly install all maintenance patches and resolutions.

SD-2.15.4.3. Good Standing

Section Effective Date: 31-Mar-2023

The provision of support by LevelBlue during the Service Term is contingent upon Customer's performance of its payment and other obligations. LevelBlue reserves the right, in addition to other remedies available, to suspend its provision of support services for so long as Customer is not current with its obligations.

Term/Abbreviation	Definition
Alarm	Alarm is a notification that a single Event or series of Events of interest have taken place that may require attention or investigation. An Alarm is based on whether certain conditions are met based on defined escalation and correlation rules. One or more rules performed by the correlation engine of the Service, which analyzes these Events for behavioral patterns. These rules look at and connect Events to assess their priority and reliability and, when the system identifies a pattern, it generates an Alarm.
Caution Mode	Occurs when the Customer environment has consumed more data than is allotted in their subscription tier.
Customer Reports	Reports generated and produced through Customer's USM Anywhere dashboard or Service reports otherwise furnished to the Customer by LevelBlue pursuant to Customer request.
Documentation	User manuals and any other materials regarding the Service, including updates thereto, in any form or medium made generally available by LevelBlue to Customers or Users, regarding the installation and use of the Service.
Event	An Event is a single activity record of traffic or a data exchange detected by the Service. Events are derived from device, system, and application logs (e.g. firewalls, operating systems, IDS, proxy servers, applications, antivirus software, etc.).
FedRAMP	FedRAMP stands for the "Federal Risk and Authorization Management Program." This government-wide program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
GSA	U.S. General Services Administration.

Term/Abbreviation	Definition
Investigation	An Investigation(s) is used to manage the full life cycle of an actionable security incident from detection to resolution. One Investigation can manage multiple related Alarms and Events. Investigations are managed and viewable from the USM Platform. The Investigation User Interface (UI) contains the Alarms and Events associated with a security incident, and "Notes" can be added describing an assessment of the threat and risk of the incident, recommendations, and the option to attach files related to the incident.
Maintenance	Maintenance time can be either for "Scheduled Maintenance" or "Emergency Maintenance". "Scheduled Maintenance" is maintenance, repair or updating activities that are performed during a maintenance window established by LevelBlue (e.g., by publishing on the USM Platform). "Emergency Maintenance" is unscheduled maintenance, repair or updating activities that are necessary in order to protect LevelBlue facilities, network services or the security of Customer equipment or property. LevelBlue will attempt to provide reasonable notice to the Customer when LevelBlue determines that it is required to perform Emergency Maintenance prior to the maintenance activity being performed.
Onboarding Email	Email sent to the Customer contact email address, defined in the Service Agreement, confirming a purchase and containing Service specific details and information necessary for commencement of purchased Service Components.
Outage	Outage is (unless stated otherwise) measured in minutes and is the time a Service or Service Component is unavailable on an unscheduled basis. An Outage does not include time when the Service or Service Component is unavailable during a scheduled period for maintenance, repair or upgrade. Customer notice of a scheduled maintenance, repair or upgrade may be given directly to Customer or by posting in USM Platform and is deemed received by Customer upon posting.
Recovery Mode	Environments in Recovery Mode will operate with no restrictions, and USM Anywhere will re-evaluate the Customer's projected monthly data consumption over a period of 24 hours.
Service Term	The Service Term means the period that Customer has the right to use the Service as set forth in the Service Agreement.
USM Anywhere	USM Anywhere^{SM} is LevelBlue's cloud-hosted security monitoring service that centralizes monitoring of networks and devices in the cloud, on premises, and in remote locations for organizations that do not require a FedRAMP approved security provider. For purposes of training, which is available for Customers to purchase as an add-on Service Component, the course materials for the Service and USM Anywhere are the same.

Term/Abbreviation	Definition
Violation Mode	Occurs when data consumption exceeds 150% of the Customer's subscription tier data allowance, or if the subscription has been in Warning Mode for two consecutive months. Violation Mode ends when Customer starts a new month (based on Customer's onboarding start date) or if Customer upgrades the subscription tier.
Warning Mode	Occurs when the Customer's data consumption has exceeded 125% of their subscription tier data allowance, or if the subscription has been in Caution Mode for more than three consecutive months.

Service Level Objectives

SLO-1. Overview

Section Effective Date: 13-Apr-2021

The Service Level Objectives (SLO) herein define the service levels that LevelBlue will endeavor to provide for the response time to Issues during the Service Term. SLOs are indicative of the service level LevelBlue strives to meet, but Customer is not entitled to receive any credits for failure to attain an SLO.

SLO-2. Contacting Support and Reporting an Issue

Section Effective Date: 13-Apr-2021

Customer may report an Issue through the Success Center at https://success.alienvault.com/ (Success Center), by phone (numbers listed here https://cybersecurity.att.com/support), or by chat (through the Success Center); provided, however, all Issues reported on Saturday or Sunday must be done through the Success Center. When reporting an Issue, Customer will include a detailed description of the Issue. Customer will report each Issue encountered by Customer separately. "Issue" means a single, reproducible issue or problem materially or significantly affecting the functionality of the Service.

SLO-2.1. Issue Classification

Section Effective Date: 13-Apr-2021

When an Issue is reported, the severity of the Issue will be classified based on the impact to Customer's business operations in accordance with the severity classification table below. To the extent that LevelBlue disagrees with any Issue classification provided by Customer, LevelBlue will promptly advise Customer of the revised

classification of any Issue and the parties will resolve through good faith negotiations any disagreement regarding classification.

SLO-3. Response Time

SLO-3.1. Standard Response Time

Section Effective Date: 13-Apr-2021

LevelBlue will use reasonable efforts to respond to each of Customer's reported Issues within the Support Hours applicable to Customer and within the timeframe designated below based on the Service purchased and Severity Level as determined by LevelBlue.

Severity Level	Definition	Response Times	Commitment
Severity 0	Entire Service, or a whole region thereof, is inaccessible or unusable while Customer's Internet is functioning properly	1 hour	LevelBlue will work on a resolution until Issue is resolved or a reasonable workaround is applied.
Severity 1	Service is up and running but multiple customers are experiencing significant issues that impact their ability to use the service	2 hour	LevelBlue will work with Customer to resolve the Issue until the Issue is fixed or a reasonable workaround is applied.
Severity 2	The issues cause significant loss of service or is a significant error. The impact is an inconvenience that may require a workaround to restore functionality or is a minor error, incorrect behavior, or a documentation error that does not impede the operation of a system.	4 hours	LevelBlue will work with Customer to mutually prioritize and schedule resolutions into regular release cycles
Severity 3	The issue causes minor reduction of service or is a minor error. The impact is an inconvenience that may require a workaround to restore functionality or is a minor error, incorrect behavior, or a documentation error that does not impede the operation of a system.	24 hours	LevelBlue will work with Customer to mutually prioritize and schedule resolutions into regular release cycles.
Severity 4	Minor defects and errors that do not impede system operation in a normal manner	36 hours	LevelBlue will work with Customer to mutually prioritize and schedule resolutions into regular release cycles.

SLO-4. LevelBlue Managed Threat Detection and Response for Government Service Level Objective

Section Effective Date: 31-Mar-2023

The performance objective for LevelBlue Managed Threat Detection and Response for Government availability is described below.

"LevelBlue Managed Threat Detection and Response for Government Availability" is measured by the following calculation:

- ((TT – TTF) / TT) x 100 = Percentage (%) of LevelBlue Managed Threat Detection and Response for Government Availability
    - TT = Total available Minutes per Month (Total minutes in a month – Maintenance = TT). Total available minutes do not include Maintenance.
    - TTF = Total Minutes of LevelBlue Managed Threat Detection and Response for Government Outage Minutes during the measurement Month.

An LevelBlue Managed Threat Detection and Response for Government Availability Outage shall occur if Customer is unable to access the USM Platform for more than a minute. LevelBlue's objective is to give customers access to the USM Platform at least 99.99% of the time.

Service Level Agreement

SLA-1. LevelBlue Managed Threat Detection and Response for Government Service Level Agreement

SLA-1.1. Overview

Section Effective Date: 31-Mar-2023

A Service Level Agreement ("SLA") is available only for time to notify the customer of Investigation Creation after an Event has been received by the platform.

SLA-1.2. SLA Exclusions

Section Effective Date: 31-Mar-2023

Notwithstanding any other clause herein, no commitment is made hereunder with respect to: (i) the Service being used in conjunction with hardware or software other than as specified in LevelBlue's published Documentation, (ii) hardware, software or

other data center equipment or services not in the control of LevelBlue or outside the scope of the Service. (iii) alterations or modifications to the Service, unless altered or modified by LevelBlue (or at the direction of or as approved by LevelBlue); (iv) defects in the Service due to accident, hardware malfunction, abuse or use other than in accordance with LevelBlue's published Documentation (unless caused by LevelBlue or its agents); (v) an evaluation of the Service or other trial provided to Customer at no charge; (vi) any problems or issues of connectivity due to the network or internet connection of Customer; or (vii) any Force Majeure event that effects the Service.

SLA-1.3. Time to Notify

Section Effective Date: 31-Mar-2023

Alarm Priority	Strategy Examples	Reporting Timeframe from Event Receipt
High	Malware Infection Privilege Escalation Data Exfiltration Vulnerable Software Exploitation	2 Hours
Medium	Brute Force Authentication Credential Abuse Phishing Code Execution	8 Hours
Low	Anomalous User Behavior Account Manipulation Service Discovery Portscan	24 Hours

The duration of time to notification will be determined by using the chart above. The SLA for Customer contact is based on the time of Event(s) receipt to Investigation creation notification.

SLA-1.4. SLA Reporting and Claims

Section Effective Date: 31-Mar-2023

Customer's sole remedy in the event it is determined that an SLA remedy is available will be a ten percent credit of the monthly recurring charge set forth in the Service Agreement for the Month in which the Investigation occurred. To file a claim, Customer must provide written notice within 30 days of the date of the notice of the Investigation which includes the following:

- Information detailing the dates and time periods for the claim.
- An explanation of the claim made under this SLA regarding time to notify.

All claims will be verified against LevelBlue's system records. Should any claim submitted by Customer be disputed, LevelBlue will make a determination in good faith based on its system logs, monitoring reports and configuration records and will provide to Customer a record of Service time to notify for the period in question upon Customer request. The record provided by LevelBlue shall be definitive. LevelBlue shall respond to a Customer claim within 10 days of claim submission.

All remedies referred to herein are subject to Customer having paid all applicable fees and fulfilled all of its obligations pertaining to the Service.

Pricing

P-1. Pricing

Section Effective Date: 31-Mar-2023

- Defined Scope. Applicable rates, prices, discounts and other terms for the Service purchased by Customer are set forth in the Service Agreement. Any additions or changes to the Service may necessitate changes in pricing.
- Customer may have separate contracts for TDR for Government, USM Anywhere, and a contract for LevelBlue Managed Threat Detection and Response for Government at the same time. If Customer chooses to transition from or between the aforementioned services, a new contract will be required.
- Any USM Anywhere services purchased through LevelBlue's affiliate, AlienVault, Inc., cannot be transferred from AlienVault to LevelBlue. Any TDR for Government services purchased through LevelBlue cannot be transferred from LevelBlue to LevelBlue's affiliate, AlienVault, Inc., and this includes any Customer Data.

P-2. Service Activation

Section Effective Date: 13-Apr-2021

LevelBlue provides activation for the Service (Service Activation). The initial Service Activation will occur on the date LevelBlue has provided the Onboarding Email to Customer (Service Activation Date).

For (a) any new Service Component purchased after the initial Service Activation Date; or (b) any change to a purchased Service Component, such as an amendment or upgrade, service activation for the new or modified Service Component will occur on the date LevelBlue has provided the Service Component Onboarding Email.

The Service Activation date for Service renewals will be the date immediately following expiration of the previous term.

P-3. Invoicing

Section Effective Date: 13-Apr-2021

Customer's obligation to pay for a Service Component begins upon the Service Activation Date.

For any new Service Component purchased after the initial Service Activation Date, Customer's obligation to pay for that Service Component will begin upon its Service Activation.

Country Specific Provisions

CSP-1. Country Specific Availability

Section Effective Date: 31-Mar-2023

The Service is only available in the United States, including Alaska, Hawaii, Puerto Rico, and Guam.

CSP-2. EU General Data Protection Regulation Requirements

Section Effective Date: 31-Mar-2023

For data protection purposes, the applicable Data Protection Agreement for this Service, including pre-populated Model Clauses, is located at https://cybersecurity.att.com/legal/gdpr/customers. The Service Guide General Provisions section "EU General Data Protection Regulation Requirements" does not apply to this Service.