SERVICE DESCRIPTION

Taegis Transition Services: Advanced

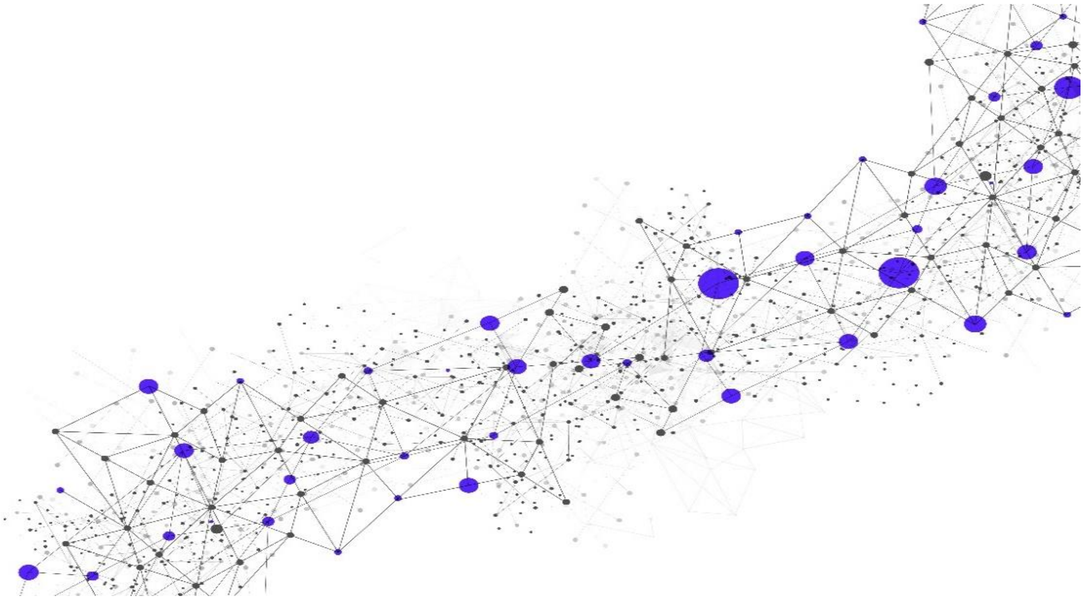
(XDR, ManagedXDR, and ManagedXDR Elite)

Release Date

December 20, 2023

Version

1.3



www.secureworks.com
A Dell Technologies Company

Global Headquarters
1 Concourse Pkwy NE #500
Atlanta, GA 30328
Phone: +1 877 838 7947
Email: info@secureworks.com
Additional office locations: https://www.secureworks.com/about/offices

Table of Contents

Copyright

Due to continued service development, the information in this publication and related software may change without notice. Please refer to your contract with Secureworks for any provided warranty information.

1 Service Introduction

This Service Description ("**SD**") describes the Taegis Transition Services: Advanced Service ("**Service**"). All capitalized words and phrases shall have the meanings set forth herein, as defined in the Glossary, or within the Secureworks-applicable agreement, such as the Customer Relationship Agreement.

1.1 Overview

Secureworks will assist Customer with transitioning from the Secureworks Counter Threat Platform ("**CTP**") to Taegis™ XDR ("**XDR**") or our managed service, Taegis ManagedXDR ("**ManagedXDR**"). Customer must purchase XDR or ManagedXDR through a separate Transaction Document. The Service includes high-level validation of Customer's environment followed by training, transition to XDR or ManagedXDR, and handover, as explained further below.

Notes:

- This Service is also available to Customer with purchase of ManagedXDR Elite through a separate Transaction Document.
- This is a per-tenant Service. If Customer has more than one tenant (i.e., **Additional Managed Tenant**) for which transition services needs to be provided, then this Service must be purchased as an add-on for each of Customer's tenants.

Secureworks will perform the following:

- Provide project and technical governance for the duration of the project to deliver a well-informed, timely transition project
- Validate the applicable portion of Customer's existing environment (the network, cloud, and endpoint infrastructure that is presently being monitored) based on Customer-provided network diagrams
- Develop the Solution Validation Document that contains details such as number of XDR collectors and custom rules, and assets for migration
- Discuss the approach to migration specifically related to re-directing the existing data sources to XDR
- Develop the Asset Migration Worksheet to identify and document the in-scope integrations for XDR/ManagedXDR (as applicable)
- Develop the Target Workflow Document to provide Customer with a view of the operational workflow with XDR/ManagedXDR
- Assist Customer with deploying XDR Collector(s) and configuring Integrations for compatible data sources (on-premises log sources and cloud Integrations)
- Provide training (remotely through teleconference) to Customer's administrators and security analysts
- Deliver Scenario-based Workshop to validate Customer's knowledge, understanding, and usage of information within XDR
- Activate the XDR/ManagedXDR Service and disable access to CTP
- Close the project after the transition is completed and conduct a handover to the Customer Success Manager ("**CSM**")

  Note: See the XDR/ManagedXDR documentation for more information about the CSM; see also the CSM description located here: https://www.secureworks.com/descriptions/customer-success-manager.

Customer will be assigned a Transition Project Manager and a Technical Consultant who will track, report, and guide Customer through the transition from CTP to XDR/ManagedXDR in an agreed-upon timely manner.

Notes:

- This Service is also referred to as a “project” within this SD.
- All project documentation and communication (including training) will be in English; provided that, customers purchasing from our Japan subsidiary may choose delivery in Japanese.
- If Customer has a need that requires significantly more work, such as a ServiceNow integration with XDR or ManagedXDR to be implemented as part of the transition, then a separate Transaction Document will be required.

The Service includes the following:

- One (1) project to transition to XDR or ManagedXDR
  - Creation of Customer’s XDR tenant (also may be referred to as Customer’s XDR instance)
  - One (1) Solution Validation Workshop
  - One (1) training session for Customer’s administrators
  - One (1) training session for Customer’s security analysts
  - Six (6) or more on-premises and cloud environments (data centers)
  - Five hundred one (501) or more monitored assets (existing non-EDR assets being monitored within CTP)
  - Up to ten (10) CTP multi-purpose logic engine (“**MPLE**”) rule conversions from CTP to XDR
  - One (1) Scenario-based Workshop
  - Collaboration with up to three (3) separate groups or teams for the project duration (i.e., Customer’s Business Units; a third party that is managing Customer’s networks, infrastructure, cloud environment)
  - Technical Governance:
    - Solution Validation Workshop
    - Guidance on Migration approach
    - Asset Qualification
  - Project Governance:
    - Commencement Meeting
    - Weekly Status Meetings
    - Project Closure Meeting
  - Onboarding of new assets (as mutually agreed in the Solution Validation Workshop(s))
  - Disable Customer’s access to CTP (Customer and Secureworks will agree on when to disable this access)

See Section 2, Service Details, for more information about the Service, including further explanation of the components listed above.

1.2 Objectives

The objectives for this Service are as follows:

- Advise on and document the approach to transition Customer from CTP to XDR/ManagedXDR using Secureworks’ transition methodology with minimal operational interruption

- Reduce time to value through an end-to-end governed transition project to support the successful transition from CTP to XDR/ManagedXDR
- Educate Customer administrators and security analysts on effective use of XDR/ManagedXDR through theoretical and interactive training
- Effective transition of the Customer's security elements comprising people, process, technology to the target XDR/ManagedXDR state
- Close all legacy CTP services and transfer Customer to Customer Success Manager for Steady State support

1.3 Customer Obligations

Customer will perform the obligations listed below and acknowledges and agrees that the ability of Secureworks to perform its obligations hereunder are dependent on Customer's compliance with these obligations. Customer will do the following:

- Assign a project lead to coordinate the activities of Customer's third-party suppliers and internal resources and work with the Secureworks project manager to coordinate all other activities for the project
- Ensure that its personnel are scheduled and available to assist as required for the Service, including being available for workshops, trainings, and meetings
- Obtain consent and authorization from the applicable third party, in form and substance satisfactory to Secureworks, to permit Secureworks to provide the Service if Customer does not own network resources such as IP addresses, Hosts, facilities or web applications
- Provide prompt responses, participate in workshops and activities for the Service, and proactively act when necessary to provide required information, required infrastructure, or personnel who will be using XDR/ManagedXDR and provide approval for successful completion of each stage of the project
- Customer personnel to provide direct support to make any changes to Customer's systems and infrastructure to enable the integrations to XDR
- Customer-scheduled interruptions and maintenance intervals will allow adequate time for Secureworks to perform the Service
- Ensure Customer's internal and third-party personnel are available and participate as required for the project
- Ensure that any Customer-supplied data and/or log sources are in a format that can be parsed by the tools used for XDR without the need for custom integration with XDR
- Complete XDR registration upon receipt of instructions from Secureworks (***Note:*** The instructions include the initial invitation to Customer's Tenant Administrator user for XDR.)
- Customer's Tenant Administrator will generate additional invitations for Customer's additional users of XDR
- Begin deploying Taegis™/Red Cloak™ endpoint agents (or other compatible endpoint agents / software) after the Commencement Meeting
- Deploy XDR Collector(s) with support from Secureworks
- Clearly communicate Customer's change management process to Secureworks (implementation of changes for this Service will occur within the required change management period to transition Customer to XDR/Managed XDR)

- Prepare any Service-specific locations, including the virtual environment(s) and any related infrastructure for XDR Collectors and detectors within XDR that are in scope for XDR/Managed XDR
- Ensure that Customer's project lead will do the following:
  - Partner with Secureworks to manage and track risks, issues, and decisions
  - Review deliverables thoroughly and notify Secureworks of any required changes or additions, or provide written acceptance of the deliverables
  - Communicate issues, concerns, and progress weekly (resource, network, device, facilities, etc.)
  - Partner with Secureworks to jointly govern the project and participate in technical work sessions as needed

2 Service Details

The subsections below contain details about the Service and how it will be implemented.

2.1 Service Implementation

The Service is delivered using the following four (4) stages:

- Validation
- Training
- Transition
- Handover

Each stage is described in the sub-sections below.

2.1.1 Validation

This stage focuses on the tasks that are required to configure Customer's XDR tenant, validate the technical elements of Customer's current monitoring environment, and understand changes in Customer's environment that impact the project.

Activity 1 – Create Taegis XDR Tenant: The Secureworks project manager will create and configure Customer's XDR tenant. The tasks include the following:

- Create/modify Customer's existing Red Cloak domain (***Note:*** This item is not applicable to the Taegis Endpoint Agent.)
- Create/modify tenant in Tenant Manager
- Create/modify Customer in Zendesk
- Provide user access to XDR for Customer's Tenant Administrator
- Install support contract and update project status

Completion Criteria: This activity is complete when Secureworks sends the introduction email to Customer's Tenant Administrator for XDR, which contains links to XDR and other relevant sources of documentation.

Activity 2 – Conduct Commencement Meeting: Secureworks will conduct an initial meeting remotely through teleconference on a mutually agreed-upon date and time to do the following:

- Begin planning for Customer's transition to XDR/ManagedXDR
- Introduce project personnel and discuss team roles and responsibilities
- Review objectives, in-scope and out-of-scope items, migration approach, and the timeline to complete the transition
- Review Customer's environment and organization, including the following:
  - Locations (such as data centers) to be considered
  - Quantity of data/log sources and integrations
- Agree on a date and time for the Solution Validation Workshop, XDR Administrator training, and the weekly status meetings

Completion Criteria: This activity is complete when the teleconference concludes and Secureworks sends an email to Customer's designated Point of Contact ("**POC**") with the documented actions and a copy of the commencement meeting presentation.

Activity 3 – Conduct Solution Validation Workshop: Secureworks will conduct this workshop remotely through teleconference on a mutually agreed-upon date and time to perform the following:

- Confirm Secureworks' understanding of: 1) Customer's current monitoring state and document changes; and 2) Customer's current security operations and document changes
- Confirm the assets that are in scope for the transition and specify:
  - Assets not currently supported by XDR
  - Assets with questionable value regarding Customer's overall security posture
- Discuss and agree on number of, and locations for, XDR Collectors
- Confirm the number of custom rules that are in use in Customer's CTP instance
- Discuss and confirm the Service migration approach from CTP to XDR

Completion Criteria: This activity is complete when Secureworks delivers the Solution Validation Workshop and sends an email to Customer's designated POC, which contains a copy of the Solution Validation Document.

Activity 4 – Establish Project and Technical Governance: The Secureworks project manager and technical consultant will govern the transition project through the effective use of the workshops, meetings and/or deliverables listed below.

Technical Governance:

- Solution Validation Workshop – Confirm the assets being monitored by CTP, the assets that should be migrated to XDR and the agreed migration approach between both platforms
- Technical/Architecture Review Board support – Development of the Solution Validation Document that will be used to obtain approval for any changes required within Customer's network
- Asset Qualification – Through a consultative approach, capture the finalized list of assets that will be migrated to XDR
- Benefits and Acceptance Document – The final project document that summarizes for primary stakeholders the project background, achievements (e.g., number of completed integrations, assets migrated), and immediate benefits of the XDR/ManagedXDR service to Customer; monitoring and operations improvements; future recommendations; project lessons learned; and Service acceptance to proceed to Steady State

Project Governance:

- Commencement Meeting – Review scope, timelines, governance and introduce the project team members
- Weekly Status Meetings – Review progress for the transition to XDR/ManagedXDR based on the defined milestones and established dates
- Project Plan – Develop this plan together, capturing activities, dependencies, and milestones to transition Customer from CTP to XDR/ManagedXDR
- Monthly Steering Meetings – Review project outcomes, escalations, primary issues, and mitigation requiring Customer stakeholder approval
- Risks, Assumptions, Issues and Dependencies ("**RAID**") Log – Maintain this log for issue and risk management so that appropriate mitigation can be established to avoid any potential impacts to the project
- Communication Plan – Capture cadence and participation of various meetings along with communication escalation information for both Customer and Secureworks project teams
- Project Closure Meeting – Obtain acceptance from Customer to formally enter Steady State and close the transition project

Completion Criteria: This activity is complete when Secureworks obtains approval to close the project after providing all the agreed deliverables to Customer.

2.1.2 Training

This stage focuses on training Customer's security analysts and administrators to use XDR and the information produced within XDR. Training is provided as indicated below.

Activity 1 – Conduct Administrator Training: Secureworks will conduct a single training session remotely through teleconference for Customer's administrators on a mutually agreed-upon date and time. Topics include the following:

- Create and configure XDR integrations
- Create and deploy XDR Collectors
- Understand Event Types and XDR Schemas
- Understand available orchestration options, searches within XDR and how to use them, and system APIs for exporting data from XDR

Completion Criteria: This activity is complete when the teleconference concludes and Secureworks sends an email to Customer's designated POC with a link to the recording of the training session.

Activity 2 – Conduct Security Analyst Training: Secureworks will conduct a single training session remotely through teleconference for Customer's security analysts on a mutually agreed-upon date and time. Topics include the following:

- Introduction to the MITRE ATT&CK framework
- Explain the Investigation workflow
- Discuss alert feedback and threat response actions, Threat Intelligence and its use in XDR, and XDR tooling and reporting
- Create custom rules and suppression

Completion Criteria: This activity is complete when the teleconference concludes and Secureworks sends an email to Customer's designated POC with a link to the recording of the training session.

2.1.3 Transition

This stage focuses on executing the approach to transition Customer from CTP to XDR/ManagedXDR. The transition is expected to follow the schedule agreed to within the established project plan.

Activity 1 – Develop Asset Migration Worksheet: Secureworks will document the following information in the Asset Migration Worksheet:

- In-scope assets (data sources) and their prioritization
- Type of data source (e.g., firewall, NGFW, DC, API, AD), and Schema it populates (e.g., Auth, NetFlow, NIDS)
- Mapping between the detectors in XDR and the data sources

Completion Criteria: This activity is complete when Secureworks sends an email to Customer's designated POC, which contains a copy of the Asset Migration Worksheet.

Activity 2 – Develop Target Workflow Document: Secureworks will conduct an interactive session with Customer to understand the differences between the CTP security monitoring workflow and the new workflow using XDR, which serves as the foundation for Customer's Target Operating Model. A summary of tasks included in this stage are as follows:

- Document (pictorial definition) Customer's current security monitoring workflow
- Document (pictorial definition) Customer's target security monitoring workflow
- Identify deficiencies between current and target workflows

Completion Criteria: This activity is complete when Secureworks delivers an email to Customer's POC with a copy of the Target Workflow Document.

Activity 3 – Provide Integration Support: Secureworks will provide support to Customer throughout the transition stage. Communication between Customer and Secureworks will be through emails and teleconferences. A summary of support tasks that Secureworks will conduct for this activity are as follows:

- Guide and assist Customer in creating XDR Collectors
- Provide guidance on direct API integrations
- Create up to the number of defined custom rules as specified within the Transaction Document
- Validate and demonstrate events and alerts from assets within XDR

Completion Criteria: This activity is complete when the in-scope assets have been migrated to XDR.

Activity 4 – Activate XDR/ManagedXDR: Secureworks will jointly work with Customer to secure approval to activate the XDR/ManagedXDR service after all the pre-requisites have been met, which include the following:

- Customer completed activities for forwarding agreed in-scope logs to XDR collector(s)
- Customer completed configuration of agreed in-scope cloud integrations
- Secureworks completed validation of agreed in-scope logs in XDR as evidenced within the Asset Migration worksheet
- Customer completed deployment of a supported endpoint agents on at least 40% of its Licensed Volume
- Customer provided three (3) escalation contacts for escalating incidents in XDR

- Customer and Secureworks agreed to plan for disabling Customer's access to CTP (***Note:*** The actual activities for disabling access to CTP are conducted immediately after activation of the XDR/ManagedXDR service.)

Completion Criteria: This activity is complete when Secureworks delivers an email informing Customer's POC that the XDR/ManagedXDR Service has been activated.

2.1.4 Handover

This stage focuses on validating that Customer's personnel can consume the information within XDR, and thereafter closing the project with Customer in the presence of the Secureworks CSM.

Activity 1 – Scenario-based Workshop: Secureworks will provide to Customer fictional scenarios based on current real-world threats (aligned with the MITRE ATT&CK framework). Using Customer's XDR tenant, Secureworks will challenge Customer's security operations personnel to demonstrate effective use of and understanding of the features and functions withing XDR. The scenarios will test the ability of Customer's personnel to perform the following tasks:

- Search for primary information and artifacts
- Create Investigations

Additionally, Secureworks will provide ad-hoc XDR training during the workshop to assist Customer's personnel in completing the tasks if necessary.

Secureworks will also create the Acceptance and Benefits Document, which will contain a final project summary based on the transition Engagement and the following information:

- Summary of Milestones, Deliverables, and Acceptance (includes transition and Service enablement dates)
- Metrics for Transition from CTP to XDR
- Primary Project Benefits from Transition
- Improvements Achieved for Customer's Security Operations (includes observations from the Threat Scenario Workshop)
- Improvements Achieved for Customer's Security Monitoring
- Items for Steady State Consideration (includes recommendations for assets to onboard in the future)

Completion Criteria: This activity is complete when Secureworks finalizes the Acceptance and Benefits Document and schedules the Project Closure Meeting with Customer.

Activity 2 – Transfer to CSM and Project Closure: Secureworks will conduct an internal meeting with Customer's CSM to review the Acceptance and Benefits Document. After the internal meeting, the Project Closure meeting will be scheduled with Customer to review the following:

- Acceptance and Benefits Document
- Summarize any remaining actions to transfer to the CSM
- Confirm Customer's acceptance into Steady State
- Obtain Customer's agreement to close the project

Completion Criteria: This activity is complete when the following occurs:

- Secureworks facilitates the Project Closure Meeting and includes Customer POC and Customer's CSM
- Secureworks completes the Project Closure Meeting and sends an email to Customer's designated POC, which contains a copy of the Project Closure Meeting presentation and the Acceptance and Benefits Document.

2.2 Service Delivery

The subsections below contain information about how Service and support are delivered to Customer.

2.2.1 High-level Project Management

Secureworks will provide a project manager to oversee management of the project for its agreed duration.

The scope of the project management includes the following:

- Act as the Secureworks project team's primary point of contact for the project
- Provide early visibility of essential Customer responsibilities and required deliverables to allow the Secureworks project team to successfully complete in-scope activities
- Engage directly with identified stakeholders for the duration of the project to ensure Customer and Secureworks are progressing with mutually agreed upon responsibilities and action items
- Initiate corrective action where required, managing risks and issues with proposed mitigation plans
- Monitor and manage the project against the established scope, to include project schedule, RAID, and quality requirements
- Obtain approval on scope definition and ensure completed deliverables are accepted by Customer

The Service(s) will be delivered remotely from a secure location. The collection of Customer information will be gathered remotely.

2.2.2 Timeline

Secureworks will use commercially reasonable efforts to meet Customer requests for dates and times to deliver the Service(s), taking into consideration Customer-designated maintenance intervals, Customer deliverable deadlines, and other Customer scheduling requests.

Secureworks will assign personnel (i.e., a project manager and a technical consultant) to this project, who are located primarily in the United States or across Europe, the Middle East, and Africa.

The project is planned for delivery within a period of twelve (12) to sixteen (16) weeks; however, Customer and Secureworks will agree to a more specific timeline with weekly milestones after the Solution Validation Workshop. If this delivery period increases due to Customer dependencies taking longer than anticipated or for other reasons beyond the control of Secureworks, then additional effort will need to be jointly approved.

All Secureworks-specific activities will be completed remotely by Secureworks personnel using effective collaboration tools to engage with Customer's personnel for the duration of the project. Secureworks personnel will collaborate with Customer's personnel during what is considered normal business hours in the regions in which the assigned Secureworks personnel reside; however, they will make every effort to accommodate Customer's time zone(s) when meetings are required.

2.2.3 Deliverables

Listed in the table below are the standard deliverables for the Service.

Stage	Deliverable Name	Delivery Method
Validation	Solution Validation Workshop	Teleconference
	Solution Validation Document	Email (document in PDF)
	Target Workflow Document	PowerPoint presentation in PDF
	RAID Log	Excel Spreadsheet
	Project Plan	Email (plan in PDF or another agreed-upon format)
	Communication Plan	Email (plan in PDF)
	Status Report (Weekly)	Email (report in PDF)
	Steering Report (Monthly)	Email (report in PDF)
Training	XDR Administrator	Teleconference
	XDR Security Analyst	Teleconference
Transition	Asset Migration Worksheet	Email (worksheet in PDF)
Handover	Scenario-based Workshop	Teleconference
	Acceptance and Benefits Document	Email (document in PDF)

2.3 Out of Scope

The information in Section 2 comprises the Secureworks standard in-scope offering for the Service. Any other services or activities not specifically listed as in scope are out of scope. Upon request, Secureworks can provide out-of-scope technical support on a time and materials basis pursuant to a separate Transaction Document.

Specific items that are out of scope include but are not limited to the following:

- Onboarding of new assets (only existing monitored assets will be transitioned)
- Tasks associated with services not listed in the Transaction Document or any other ordering document for XDR/ManagedXDR
- Activities not required for integrating and delivering XDR/ManagedXDR as agreed
- Use of the Secureworks Project Manager to manage Customer's or Customer's third-party activities or resources

Secureworks reserves the right to decline requests that:

- Are beyond the scope of the Service(s) described herein

- Are beyond the capability of Secureworks to deliver within the contracted service levels
- Might violate legal or regulatory requirements

3 Service Fees and Related Information

Service Fees are based on a fixed fee; Customer is billed upon execution of a Transaction Document. See Customer's MSA or CRA (as applicable) and Customer's Transaction Document for details, including the following:

- Billing and Invoicing
- Out-of-Pocket Expenses
- Services Term

3.1 Invoice Commencement and Related Information

See the Service-specific Addendum or Customer's Transaction Document for information about invoice commencement.

3.2 Out-of-Pocket Expenses

The Service fees outlined above include all incidental out-of-pocket expenses such as report preparation and reproduction, faxes, copying, etc.

The following out-of-pocket expenses are NOT included in the Service fees: those travel fees related to transportation, meals and lodging to perform the Services. Customer agrees to reimburse Secureworks for all reasonable and actual out-of-pocket expenses incurred for travel to the Customer location in the performance of the Services herein.

These out-of-pocket expenses are only applicable if Customer requests on-site service.

4 Additional Considerations and Information

4.1 Record Retention

Secureworks will retain a copy of the Customer Reports and supporting Customer Data in accordance with Secureworks' record retention policy, which provides such retention for a period commensurate with the usefulness of such Customer Reports and supporting Customer Data, subject to any applicable legal or regulatory requirements.

Unless Customer gives Secureworks written notice to the contrary prior thereto, then thirty (30) days after delivery of its final report, Secureworks shall have the right, in its sole discretion, to dispose of all acquired hard drive images and other report backup information acquired in connection with its performance of its obligations under this service description.

5 Glossary

Term	Description
Additional Managed Tenant	An add-on service for ManagedXDR and ManagedXDR Elite that provides Customer with more than one XDR tenant.