Cisco Business Critical Services

Services for Operations

This document contains the detailed description of capabilities and Deliverables aligned to Cisco Business Critical Services for Operations.

Note: This document must be read in conjunction with the Cisco Business Critical Services General Terms.

Navigation Links:

Document Name	Link
Cisco Business Critical Services General Terms	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_General_Terms.pdf
Cisco Business Critical Services for Operations	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Operations.pdf
Cisco Business Critical Services for Engineering	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Engineering.pdf
Cisco Business Critical Services for Architecture	https://www.cisco.com/c/dam/en_us/about/doing_business/legal/service_descriptions/docs/Cisco_Business_Critical_Services_for_Architecture.pdf

TABLE OF CONTENTS

SERVICES FOR OPERATIONS OVERVIEW

Cisco Business Critical **Services for Operations** provides capabilities and Deliverables in support of availability, performance, security compliance, and management of Cisco infrastructure and application environment. Deliverables described in the Services for Operations theme are aligned by capabilities, and supported technologies, Solutions or architectures.

SERVICES FOR OPERATIONS CAPABILITIES AND DELIVERABLES

Services for Operations capabilities and Deliverables assist Customers with optimizing operations and management of the Network infrastructure and application technologies.

1. OPERATIONAL ANALYTICS

Operational Analytics assists Customer with analysis, insights and recommendations into system, Software, and operational gaps that must be addressed to optimize performance, availability, and security of the Cisco Network and application architecture.

SECTION NAVIGATION

Operational Analytics includes the following Service components, each bookmarked for easier navigation:

1.1. Platform Insights

Platform Insights identifies deficiencies and potential risks that should be resolved to optimize availability, stability, and performance of Customer's Cisco infrastructure and application environment. The Service also helps assess the effectiveness of the Cisco environment for purposes of planning current and future changes based on Customer's evolving business imperatives and requirements.

The Service involves collection and analysis of data on post-deployment or audited environments that require regularly planned or additional examination, guided by Customer needs and concerns.

Exclusions

**Specific to Wireless Networking*

- Cisco Meraki™ networking is not supported.

**Specific to Computing Systems*

- Cisco HyperFlex® is not supported.

**Specific to Data Center Switching*

- Cisco Application Control Engine (ACE) is not supported.

**Specific to Automation, Integration and Management*

- Cisco CloudCenter™ (CCC) is not supported.

**Specific to Security Policy and Access*

- Cisco Firepower® Management Center (FMC), and Identity Services Engine (ISE) are not supported.

1.1.1. Platform Insights, Type 1 - Manual or Cisco Data Collection Tool Delivered Reports

Platform Insights Type 1 provides the following reports:

- Type 1 – Configuration Best Practices
- Type 1 – Hardware Lifecycle Milestones
- Type 1 – Diagnostic Analysis
- Type 1 – Field Notices (where applicable)
- Type 1 – Audit

1.1.1a. Type 1 – Configuration Best Practices

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Data Center Orchestration and Automation
- Unified Communications
- Customer Care
- Network Security
- Cloud Security
- Video Collaboration
- Cloud Meetings and Messaging
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

- Network Management and Orchestration
- Computing Systems

Deliverables

- Type 1 Configuration Best Practices Report

Limitations

**Specific to Routing and Switching*

- Questionnaire and/or worksheet are the only data collection methods supported for gathering information as input to the Configuration Best-Practices Report.
- One (1) Configuration Best Practices Report supports up to five (5) device configurations.

**Specific to Optical Networking*

- One (1) Configuration Best Practices Report supports up to fifty (50) device configurations.
- Scope of Configuration Best Practices Report is limited to optical power level thresholds only.

**Specific to Virtual Packet Core*

- For Virtual Packet Core Solution, one (1) Configuration Best Practices Report supports up to five (5) device configurations.

1.1.1b. Type 1 – Hardware Lifecycle Milestones

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Deliverables

- Type 1 Hardware Lifecycle Milestones Report

Limitations

**Specific to Routing and Switching*

- Questionnaire and/or worksheet are the only data collection methods supported for gathering information as input to the Hardware Lifecycle Milestones Report.
- One (1) Hardware Lifecycle Milestone Report supports a maximum of one hundred (100) devices.

**Specific to Optical Networking*

- One (1) Hardware Lifecycle Milestone Report supports a maximum of fifty (50) devices.

1.1.1c. Type 1 – Diagnostic Analysis

Technologies Supported

- Optical Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core

Cisco Responsibilities

- Analyze Customer device diagnostic information to identify potential risks.

Additional Cisco Responsibilities

**Specific to Packet Core, Virtual Packet Core Solution excluding Computing Systems and Data Center Switching*

- Analyze syslog information to develop recommendations based on the following:
- Syslog event correlation, mobility packet core health information and baseline metrics

**Specific to Optical Networking*

- Analyze syslog information to develop recommendations based on the following:
- Alarms and conditions, system resources and shelf environment

Deliverables

- Type 1 Diagnostic Analysis and Recommendation Report

Limitations

**Specific to Optical Networking*

- One (1) Diagnostic Analysis and Recommendation Report supports a maximum of fifty (50) devices.
- Scope of Diagnostic Analysis and Recommendation Report is limited to alarm and circuit information, user activities, provisioning, and maintenance access information.

1.1.1d. Type 1 – Field Notices (where applicable)

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core

Deliverables

- Type 1 Field Notice Analysis and Recommendation Report

Limitations

**Specific to Routing and Switching*

- Questionnaire and/or worksheet are the only data collection methods supported for gathering information as input to the Field Notice Analysis and Recommendation Report.
- One (1) Field Notice Analysis and Recommendation Report supports a maximum of one hundred (100) devices.

**Specific to Optical Networking*

- One (1) Field Notice Analysis and Recommendation Report supports a maximum of fifty (50) devices.

1.1.1e. Type 1 – Audit

Technologies Supported

- Optical Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Unified Communications
- Video Collaboration
- Customer Care
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core
- Network Function Virtualization Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- SP Analytics and Assurance
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems

Cisco Responsibilities

- Analyze information that may include, but is not limited to:
- Performance, and tuning recommendations.
- Resource utilization analysis for planning purposes.
- Recommend areas that need further analysis, such as architecture and design or alignment of policies and standards.

Additional Responsibilities

**Specific to Application Centric Infrastructure*

- Gather Customer's working practices for maintaining ACI architecture.
- Align applicable leading-practice architecture.

Excluded Responsibilities

**Specific to Computing Systems, Data Center Switching*

- The audit analysis and report do not address:
    - Stability, performance, and tuning recommendations.
    - Resource utilization analysis for planning purposes.

Deliverables

- Type 1 Audit Report

Customer Responsibilities

- Complete platform audit questionnaire and/or worksheet, if applicable.
- Perform any necessary pre-audit steps requested by Cisco to ensure that all data is accessible during the audit.
- Provide notification of any delay in scheduled changes during the audit process.

Limitations

**Specific to Network Security, Cloud Security, Security Policy and Access, Advanced Threat*

- Type 1 Audit Report is limited to:
    - Up to one (1) Solution set or one (1) complex system (e.g., Cisco Identity Services Engine (ISE), Cisco Secure Access Control System (ACS), 802.1x deployments).
    - Up to twenty (20) devices.

**Specific to Data Center Switching*

- One (1) Type 1 Audit Report is limited to Cisco Nexus® family switches in a single instance of Data Center.

**Specific to Optical Networking*

- One (1) Type 1 Audit Report supports a maximum of fifty (50) devices.
- Scope of Type 1 Audit Report is limited to IP Addressing and Data Communications Network (DCN), and Dense Wave Division Multiplexing (DWDM) channel utilization.

**Specific to NFVI, SAE, MSX*

- Type 1 Audit Report is limited to:
    - Resource utilization analysis of CPU utilization, memory, status of the services running for planning purposes.

1.1.2. Platform Insights, Type 2 – Cisco Cloud Hosted Analytics Enabled and Expert Delivered Features

Exclusions

**Specific to Computing Systems*

- UCS C-Series servers not connected to Fabric Interconnect are not supported by Platform Insights Analytics Enabled Type 2 Deliverables.

**Specific to Packet Core, Mobility Policy and Access*

- Cisco Ultra Packet Core is not supported by Platform Insights, Type 2

Deliverables

Platform Insights Type 2 provides the following features and reports:

- Type 2 Configuration Best Practices
- Type 2 Hardware Lifecycle Milestones
- Type 2 Diagnostic Analysis
- Type 2 Field Notices
- Type 2 Audit Report
- Type 2 Optional: Third Party Support

1.1.2a. Type 2 – Standard Hosted Analytics Enabled and Expert Delivered Feature: Configuration Best Practices

Technologies Supported

- Routing and Switching
- Wireless Networking
- Packet Core
- Network Security
- Data Center Switching
- Storage Area Networking
- Application Centric Infrastructure
- Mobility Policy and Access
- Unified Communications

Solutions Supported

- Virtual Packet Core
  - Data Center Switching
- Software Defined Access
  - Routing and Switching
  - Wireless Networking

Deliverables

- Type 2 Configuration Best Practices

Limitations

**Specific to Wireless Networking*

- Type 2 Feature: Configuration Best Practices is supported only for Cisco Autonomous Access Points.

**Specific to Network Security*

- Type 2 Configuration Best Practices is supported only for Cisco Adaptive Security Appliance (ASA).

**Specific to Unified Communications*

- Type 2 Feature: Configuration Best Practices is supported only for Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways, and Cisco Session Management Edition.

1.1.2b. Type 2 – Standard Hosted Analytics Enabled and Expert Delivered Feature: Hardware Lifecycle Milestones

Technologies Supported

- Routing and Switching
- Wireless Networking
- Computing Systems
- Data Center Switching
- Storage Area Networking
- Network Security
- Security Policy and Access
- Unified Communications

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Deliverables

- Type 2 Hardware Lifecycle Milestones

Limitations

**Specific to Network Security, Security Policy and Access*

- Type 2 Hardware Lifecycle Milestones is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

**Specific to Unified Communications*

- Type 2 Hardware Lifecycle Milestones is supported only for Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways, and Cisco Session Management Edition and select endpoints.

1.1.2c. Type 2 – Standard Hosted Analytics Enabled and Expert Delivered Feature: Diagnostic Analysis

Technologies Supported

- Routing and Switching
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Network Security
- Packet Core
- Mobility Policy and Access
- Unified Communications

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Additional Responsibilities

**Specific to Routing and Switching, Data Center Switching*

- Provide device crash factors for top impacted devices.

**Specific to Application Centric Infrastructure*

- The following diagnostic insights are provided:

- Events, faults, audits, end-point moves, and capacity utilization.

**Specific to Packet Core, Mobility Policy and Access*

- The following diagnostic insights packages are provided:

For Base package:

- Network health summary for GTPC call flows, KPIs, and procedures such as Attach, PDP/Bearer Creation, Routing Area/Tracking Area Update, Paging, Service Requests and Handover Requests where applicable.
- Resource level summary of CPU and memory utilization.
- Session and throughput trends, resource utilization.
- Congestion packet drops, retransmissions, timeouts for all interfaces and Access Point Names (APNs).
- Interface level summary of sessions, transactions, diameter call flows where applicable.
- Syslog summary of Top N syslog events, critical, error and info syslog event trends.

Deliverables

- Type 2 Diagnostic Analysis

Limitations

**Specific to Network Security*

- Type 2 Diagnostic Analysis is supported only for Cisco Adaptive Security Appliance (ASA).

**Specific to Unified Communications*

- Type 2 Diagnostic Analysis is supported only for Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways, and Cisco Session Management Edition and select endpoints.

1.1.2d. Type 2 – Standard Hosted Analytics Enabled and Expert Delivered Feature: Field Notices

Technologies Supported

- Routing and Switching
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Security Policy and Access
- Unified Communications

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
- Software Defined Access
  - Routing and Switching
  - Wireless Networking
  - Security Policy and Access

Deliverables

- Type 2 Field Notice Analysis and Recommendation

Limitations

**Specific to Network Security, Security Policy and Access*

- Type 2 Field Notices is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

Specific to Unified Communications

- Type 2 Field Notices is supported only for Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways, and Cisco Session Management Edition and select endpoints.

1.1.2e. Type 2 – Audit Report

Technologies Supported

- Routing and Switching
- Computing Systems
- Data Center Switching
- Storage Area Networking
- Network Security
- Security Policy and Access
- Unified Communications
- Packet Core
- Mobility Policy and Access

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Cisco Responsibilities

- Analyze information which may include, but is not limited to:
- Stability, performance, and tuning recommendations.
- Resource utilization analysis for planning purposes.
- Recommendation related to areas that need further analysis, such as architecture and design or alignment of policies and standards.

Specific to Unified Communications

- Type 2 Audit Report is provided once per quarter up to four reports per year.

Excluded Responsibilities

Specific to Computing Systems, Data Center Switching, Virtual Packet Core Computing Systems, and Data Center Switching

- The audit analysis and report do not address:
- Stability, performance, and tuning recommendations.
- Resource utilization analysis for planning purposes.

Deliverables

- Type 2 Audit Report

Limitations

Specific to Data Center Switching

- One (1) Type 1 Audit Report is limited to Nexus family switches in a single instance of Data Center.

Specific to Network Security, Security Policy and Access

- Type 2 Audit Report is limited to:
- Up to one (1) Solution set or one (1) complex system (e.g., Cisco Identity Services Engine (ISE), Cisco Secure Access Control System (ACS), 802.1x deployments).

- Up to twenty (20) devices.

**Specific to Unified Communications*

- Type 2 Audit Report is supported only for Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways, and select endpoints.

1.1.2f. Type 2 – Optional Hosted Analytics Enabled and Expert Delivered Feature: Third Party Support

Third Party Support assists Customer with an inventory view of the Cisco supported third-party platforms and operating systems via Cisco Cloud Hosted Analytics.

Limitations

- SNMP MIB-2 support by the third-party device vendor is required to collect inventory data. The accuracy and completeness of the data collected by Cisco is dependent on the third-party vendor support for SNMP MIB-2.
- Cisco is not responsible for the appropriateness and reliability of any information collected or provided by a third-party vendor's device(s), website or any other sources of information.
- Cisco is not responsible for the availability, performance, security or reliability of third-party devices Customer requests Cisco to collect data and report on.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Security

Third Party Operating Systems and Platforms Supported

Company	Operating Systems	Platforms Supported
Adtran	AOS	Adtran – NetVanta 3200
Alcatel	SROS	Alcatel 7750 Services Routers
Alteon	AlteonOS	Alteon Application Switch 2208
Arista	EOS	Arista 7050 Switches
Aruba	Aruba OS	Aruba Wireless Line Controller
BoSS	BoSS	BS470-48T, ERS4550T, BS551048T
Checkpoint	IPSO GAIA	Checkpoint Firewall IPxxx
Extreme	EXOS	Extreme Summit Switches
Forti	FortiOS	Forti – Analyzer 60D, Manager
F5	TMOS	F5 – VIPRION C2400 Series, BIG IP
Huawei	VRP	Huawei S3328 Switches
Infoblox	NIOS	Infoblox 1552-A
Juniper	JunOS ScreenOS	Juniper - M Series, SRX240 Services Gateway, EX2200 Juniper Netscreen SSG5 Firewall
NetScaler	NetScalerOS	Citrix NetScaler, NetScaler SDX

Cisco Responsibilities

- Provide an inventory view of Customer third-party devices within Hosted Analytics, which may include the following:
  - Chassis, IP Address, device type, device name, software / firmware versions

Deliverables

- Type 2 Optional Third Party Inventory Report

Customer Responsibilities

- Customer is responsible for resolving data issues with data collected by Cisco from the third-party device vendor.
- In order for Cisco to provide this Service, Customer is responsible for providing expertise on third-party vendor's platforms such as but not limited to:
  - Hardware nomenclature
  - Features and configuration commands
  - Software versions
  - Access methods and credentials
- Customer must maintain and monitor the availability, performance, security and reliability of third-party devices supported by Cisco data collection method; including ensuring configurations and software versions on third-party devices deployed in the Customer environment are not misconfigured or contain defects which are affected by Cisco data collection methods.
- Customer should contact Cisco Sales representative for additional third-party platforms and features not currently listed.

1.1.3. Platform Insights, Type 3 – Cisco OnPrem Analytics and Insights Tool Delivered Reports

Platform Insights Type 3 provides the following reports and technologies supported:

- Type 3 Configuration Best Practices Report
- Type 3 Hardware Lifecycle Milestones Report
- Type 3 Product Security Advisory Customer Impact Assessment Report
- Type 3 Diagnostic Analysis Report
- Type 3 Audit Report

1.1.3a. Type 3 – Configuration Best Practices Report

Technologies Supported

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Software Defined Access
  - Routing and Switching
  - Security Policy and Access
- Virtual Packet Core
  - Packet Core

Deliverables

- Type 3 Configuration Best Practices Report

Limitations

**Specific to Network Security, Security Policy and Access*

- Type 3 Configuration Practices Report is supported only for Cisco Adaptive Security Appliance (ASA).

**Specific to Virtual Packet Core*

- Type 3 Configuration Best Practices Report is supported only for Cisco Ultra-M Solution.
- Cisco Nexus and Catalyst® Switches which are part of the Cisco Ultra-M Solution are supported.

1.1.3b. Type 3 – Hardware Lifecycle Milestones Report

Technologies Supported

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Software Defined Access
  - Routing and Switching
  - Security Policy and Access

Deliverables

- Type 3 Hardware Lifecycle Milestones Report

Limitations

**Specific to Network Security, Security Policy and Access*

- Type 3 Hardware Lifecycle Milestones Report is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

1.1.3c. Type 3 – Field Notices

Technologies Supported

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Software Defined Access
  - Routing and Switching
  - Security Policy and Access

Deliverables

- Type 3 Field Notice Analysis and Recommendation Report (where applicable)

Limitations

**Specific to Network Security, Security Policy and Access*

- Type 3 Field Notice Analysis and Recommendation Report is supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

1.1.3d. Type 3 – Diagnostic Analysis Report

Solutions Supported

- Virtual Packet Core
  - Packet Core

Deliverables

- Type 3 Diagnostic Analysis Report

Limitations

- **Specific to Virtual Packet Core*
- Type 3 Diagnostic Analysis Report is supported only for Cisco Ultra-M Solution.
- Cisco Nexus and Catalyst Switches which are part of the Cisco Ultra-M Solution are supported.

1.1.3e. Type 3 – Audit Report

Solutions Supported

- Virtual Packet Core
  - Packet Core

Deliverables

- Type 3 Audit Report

Limitations

**Specific to Virtual Packet Core*

- Type 3 Audit Report is supported only for Cisco Ultra-M Solution.
- Cisco Nexus and Catalyst Switches which are part of the Cisco Ultra-M Solution are supported.

1.2. Software Lifecycle Management (SLM)

Software Lifecycle Management assists Customer with preparing and planning future Software release decisions such as feature functionality, third-party compatibility, and release stability, aligned with Customer's future Software release objectives. It analyzes Customer's current practices related to establishing and managing release standards, working to identify risks and recommendations to help prevent potential issues.

General Limitations

The following limitations apply specifically to bugs identified in Production Software Maintenance Updates (SMUs) by Software Lifecycle Management Deliverables described below and Cisco's discretion regarding requests for and delivery of Production SMUs:

- Production Software Maintenance Updates (SMU) are provided on Customer request on supported maintenance releases for service impacting issues observed in production or during maintenance release validation, for which there is no feasible workaround.
- Software bugs identified through software recommendations or Bug Search Tools are not a basis for Production SMU request.
- Cisco reviews software bugs affecting supported maintenance releases and provides Proactive Production SMU requests when Cisco deems necessary.
- Cisco reserves the right to maintain strict control over Production SMU delivery.

Exclusion

**Specific to Wireless Networking*

- Cisco Meraki networking is not supported.

**Specific to Computing Systems*

- Cisco HyperFlex is not supported.

**Specific to Data Center Switching*

- Cisco Application Control Engine (ACE) is not supported.

1.2.1. SLM, Type 1 – Manual or Cisco Data Collection Tool-Delivered Reports

Software Lifecycle Management Type 1 consists of the following three (3) areas of focus:

- Type 1 Software Management Process and Procedure Development
- Type 1 Software Release Standards and Conformance
- Type 1 Software Risk Management and Insights

1.2.1a. Type 1 – Software Management Process and Procedure Development

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Network Management and Orchestration
- Data Center Orchestration and Automation
- Unified Communications
- Video Collaboration
- Customer Care
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Next Gen Cable Access
- SP Video Infrastructure
- IoT Edge and Fog Compute
- Industrial Networking and Collaboration

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- SP Analytics and Assurance
  - Network Management and Orchestration
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems

Cisco Responsibilities

- Collaborate with Customer to develop the Software Management Process and Procedure Document, which may include:
  - Software strategy, process, procedure, and Documentation related to Software selection.
  - Feature requirements and objectives.
  - Upgrade planning and migration triggers, such as Software advisories, Software deferrals, Software end-of-sale (EOS), Software end-of-life (EOL), and Field Notices.

Deliverables

- Type 1 Software Management Process and Procedure Document

1.2.1b. Type 1 – Software Release Standards and Conformance

Software Release Standards and Conformance consists of the following two (2) reports described below:

- Type 1 Software Analysis and Release Standards Report
- Type 1 Software Track Conformance Report

b-1. Type 1 – Software Analysis and Release Standards Report

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Data Center Switching
- Storage Area Networking
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Unified Communications
- Customer Care
- Cloud Security
- Video Collaboration
- Cloud Meetings and Messaging
- Network Security
- Security Policy and Access
- Advanced Threat
- Next Gen Cable Access
- SP Video Infrastructure
- IoT Edge and Fog Compute
- Industrial Networking and Collaboration

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
  - Packet Core

Cisco Responsibilities

- Develop the Software Analysis and Release Standards Report, which may include:
  - Overall Software recommendation(s) that Customer should test and consider.
  - Descriptions of new Software features and Hardware compatibility.
  - Unresolved Software bugs to which Customer may be exposed and, if possible, appropriate workarounds.
  - Software feature upgrade analysis based on information gathered and analysis of findings of identified Software versions relative to Customer's current and future Software feature requirements.

Deliverables

- Type 1 Software Analysis and Release Standards Report.
- Note: One (1) quantity of this Deliverables is for one (1) platform and its software release.

Limitations

- **Specific to Data Center Orchestration and Automation*
- The Type 1 Software Analysis and Release Standards Report is supported for Cisco CloudCenter only.

b-2. Type 1 – Software Track Conformance Report

Technologies Supported

- Optical Networking
- Network Security

- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Video Collaboration
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Next Gen Cable Access
- SP Video Infrastructure
- IoT Edge and Fog Compute

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Cisco Responsibilities

- Baseline Customer's release standards and conformance of deployed release standards against Cisco-recommended Software release standards.

Limitations

- **Specific to Data Center Orchestration and Automation*
- The Type 1 Software Track Conformance Report is supported for Cisco CloudCenter only.

Deliverables

- Type 1 Software Track Conformance Report

1.2.1c. Type 1 – Software Risk Management and Insights

Software Risk Management and Insights consists of the following two (2) reports described below:

- Type 1 Product Security Advisory Customer Impact Assessment
- Type 1 Software Lifecycle Milestones

Type 1 – Product Security Advisory Customer Impact Assessment

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
- SP Analytics and Assurance
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems

- Packet Core
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems

Cisco Responsibilities

- Perform the following Customer impact assessment when applicable for a published Cisco Product Security Advisory:
- Identify list of devices affected or potentially.
- Provide analysis and recommendations to address how the Cisco Product Security Advisory may impact Customer's existing deployed Solution.
- Provide recommended Software version where the fix for the Cisco Product Security Advisory is incorporated.

Additional Responsibilities

**Specific to Virtual Packet Core*

- This deliverable supports RedHat Openstack and RedHat Operating System (OS) software components.

Deliverables

- Type 1 Product Security Advisory Customer Impact Assessment Report

Type 1 – Software Lifecycle Milestones

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- SP Video Infrastructure
- Next Gen Cable Access

Solutions Supported

- Software Defined WAN
  - Routing and Switching
- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Cisco Responsibilities

- Perform the following when applicable:
- Identify devices affected by Software deferral, Software EOS, and Software EOL that are applicable to Customer's deployed Software standards and could result in a migration trigger.

Deliverables

- Type 1 Software Lifecycle Milestones Report

1.2.2. SLM, Type 2 – Cisco Cloud Hosted Analytics Enabled and Expert Delivered Features

Exclusions

**Specific to Computing Systems*

- UCS C-Series servers not connected to Fabric Interconnect are not supported by Software Lifecycle Management, Type 2 Deliverables.

Limitations

**Specific to Network Security, Security Policy and Access*

- Type 2 Software Lifecycle Management features are supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).
- ISE is not supported for Type 2 Software Analysis and Release Standards and Type 2 Software Adoption Trends.

**Specific to Unified Communications*

- Type 2 Software Lifecycle Management features are supported only for Cisco Unified Communications, Cisco Unity Connection, Cisco Instant Messaging & Presence, Cisco Emergency Responder, Cisco Voice Gateways, and Cisco Session Management Edition.

Software Lifecycle Management Type 2 consists of the following three (3) areas of focus:

- Type 2 Software Management Process and Procedure Development
- Type 2 Software Release Standards and Conformance
- Type 2 Software Risk Management and Insights

1.2.2a. Type 2 – Software Management Process and Procedure Development

Technologies Supported

- Routing and Switching
- Wireless Networking
- Unified Communications
- Network Security
- Security Policy and Access

Cisco Responsibilities

- Collaborate with Customer to develop the Software Management Process and Procedure Document, which may include:
  - Software strategy, process, procedure, and Documentation related to Software selection.
  - Feature requirements and objectives.
  - Upgrade planning and migration triggers, such as Software advisories, Software deferrals, Software EOS, Software EOL, and Field Notices.

Deliverables

- Type 2 Software Management Process and Procedure Document

Customer Responsibilities

- Share the current practices and Documentation related to establishing, complying, and managing Software release standards and Software migration triggers.

1.2.2b. Type 2 – Software Release Standards and Conformance

Type 2 Software Release Standards and Conformance consists of the following features and report described below:

- Type 2 Software Analysis and Release Standards

- Type 2 Software Track Conformance
- Type 2 Software Adoption Trends

Type 2 – Software Analysis and Release Standards

Technologies Supported

- Routing and Switching
- Wireless Networking
- Storage Area Networking
- Data Center Switching
- Network Security
- Security Policy and Access
- Unified Communications
- Packet Core
- Mobility Policy and Access

Solutions Supported

- Virtual Packet Core
  - Packet Core
  - Computing Systems
  - Data Center Switching
- Software Defined Access
  - Routing and Switching
  - Wireless Networking
  - Security Policy and Access

Note: Platforms not supported by Hosted Cloud Analytics are supported by the Software Analysis and Release Standards Report.

Cisco Responsibilities

- Analysis of Customer-specific tracks and deployed Software release standards.
- Overall Software recommendation(s) that Customer should test and consider.
- Descriptions of new Software features.
- Identify unresolved Software bugs to which Customer may be exposed and, if possible, appropriate workarounds.
- Software feature upgrade analysis of identified Software versions relative to the Customer's current and future Software feature requirements.

Deliverables

- Type 2 Software Analysis and Release Standards Report
- One (1) quantity of this Deliverables is for one (1) platform and its software release

Limitations

**Specific to Wireless Networking, Computing Systems, Storage Area Networking, Data Center Switching, Virtual Packet Core Computing Systems and Data Center Switching*

- Software analysis and release standards is delivered via a report.

Type 2 – Software Track Conformance

Technologies Supported

- Routing and Switching
- Wireless Networking
- Unified Communications
- Network Security
- Security Policy and Access

Solutions Supported

- Software Defined Access
  - Routing and Switching

- Wireless Networking
- Security Policy and Access

Cisco Responsibilities

- Assist Customer in creating groups of Software versions to be tracked.
- Baseline of Customer's release standards and conformance of deployed release standards against Cisco-recommended Software release standards.

Deliverables

- Type 2 Software Track Conformance

Limitations

**Specific to Wireless Networking*

- Type 2 Software Track Conformance feature is not available for Cisco AP-LWAN devices.

Type 2 – Optional Feature: Software Adoption Trends

Technologies Supported

- Routing and Switching
- Optical Networking
- Network Security
- Security Policy and Access

Cisco Responsibilities

- Software release upgrade trends observed in the Customer's install base.

Deliverables

- Type 2 Optional Feature: Software Adoption Trends

1.2.2c. Type 2 – Software Risk Management and Insights

Type 2 Software Risk Management and Insights consist of the following features described below:

- Type 2 Product Security Advisory Customer Impact Assessment
- Type 2 Software Lifecycle Milestones
- Type 2 Critical Bug Notification
- Type 2 Software Maintenance Update Notification
- Type 2 Optional Software Release Bug Tracking

c-1. Type 2 – Product Security Advisory Customer Impact Assessment

Technologies Supported

- Routing and Switching
- Wireless Networking
- Storage Area Networking
- Unified Communications
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching
- Software Defined Access
  - Routing and Switching
  - Wireless Networking
  - Security Policy and Access

Cisco Responsibilities

- Perform the following customer impact assessment when applicable for a published Cisco Product Security Advisory:
  - Identify list of devices affected or potentially affected.
- Provide analysis and recommendations to address how the Cisco Product Security Advisory may impact Customer's existing deployed Solution.
- Provide recommended Software version where the fix for the Cisco Product Security Advisory is incorporated.

Deliverables

- Type 2 Product Security Advisory Customer Impact Assessment

Type 2 – Software Lifecycle Milestones

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Virtual Packet Core
  - Computing Systems
  - Data Center Switching

Cisco Responsibilities

- Identify devices affected by Software deferral, Software EOS, and Software EOL that are applicable to Customer's deployed Software standards and could result in a migration trigger.

Deliverables

- Type 2 Software Lifecycle Milestones

Type 2 – Optional Critical Bug Notification

Technologies Supported

- Routing and Switching
- Network Security
- Security Policy and Access
- Unified Communications
- Packet Core
- Mobility Policy and Access

Solutions Supported

- Software Defined Access
  - Routing and Switching
  - Security Policy and Access
- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Provide Critical Bug Notification alerting the Customer of discovery, status change, or resolution of critical bugs in preferred Software release tracks.

Deliverables

- Type 2 Optional Critical Bug Notification
- One (1) quantity of this Deliverables is for one (1) platform and its software release.

Limitations

**Specific to Packet Core, Mobility Policy and Access, Virtual Packet Core*

- Type 2 Optional Critical Bug Notification is supported only for Cisco Ultra-M with Cisco Virtualized Infrastructure Manager.

Type 2 – Optional Software Maintenance Update Notification

Technologies Supported

- Routing and Switching

Cisco Responsibilities

- Provide Software Maintenance Update Notification alerting the Customer of the availability of a patch or maintenance Update for a specific bug, feature, or Software release.

Deliverables

- Type 2 Optional Software Maintenance Update Notification
- One (1) quantity of this Deliverables is for one (1) platform and its software release.

Type 2 – Optional Software Release Bug Tracking

Technologies Supported

- Routing and Switching
- Network Security
- Security Policy and Access
- Unified Communications
- Packet Core
- Mobility Policy and Access

Solutions Supported

- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Provide periodic insights and tracking of critical bugs for specified Software release standards.

Deliverables

- Type 2 Optional Software Release Bug Tracking

1.2.3. SLM, Type 3 – Cisco OnPrem Analytics and Insights Tool-Delivered Reports

Limitations

**Specific to Network Security, Security Policy and Access*

- Type 3 Software Lifecycle Management reports are supported only for Cisco Adaptive Security Appliance (ASA), Firepower, Firepower Threat Defense (FTD), and Identity Services Engine (ISE).

Software Lifecycle Management Type 3 is provided via Cisco OnPrem Analytics Tool, and consists of the following three (3) areas of focus:

- Type 3 Software Management Process and Procedure Development
- Type 3 Software Release Standards and Conformance
- Type 3 Software Risk Management and Insights

1.2.3a. Type 3 – Software Management Process and Procedure Development

Technologies Supported

- Routing and Switching
- Network Security
- Security Policy and Access

Cisco Responsibilities

- Collaborate with the Customer to develop the Software Management Process and Procedure Document, which may include:
  - Software strategy, process, procedure, and Documentation related to Software selection.
  - Feature requirements and objectives.
  - Upgrade planning and migration triggers, such as Software advisories, Software deferrals, Software EOS, Software EOL, and Field Notices.

Deliverables

- Type 3 Software Management Process and Procedure Document

1.2.3b. Type 3 – Software Release Standards and Conformance

Type 3 Software Release Standards and Conformance consists of the following reports described below:

- Type 3 Software Track Conformance Report
- Type 3 Software Analysis and Release Standards Report

Technologies Supported

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Software Defined Access
  - Routing and Switching
  - Security Policy and Access

Cisco Responsibilities

- Baseline Customer's release standards and conformance of deployed release standards against Cisco-recommended Software release standards.
- Develop the Software Analysis and Release Standards, which may include:
  - Overall Software recommendation(s) that Customer should test and consider.
  - Descriptions of new Software features and Hardware compatibility.
  - Unresolved Software bugs to which Customer may be exposed and, if possible, appropriate workarounds.
  - Software feature upgrade analysis based on information gathered and analysis of findings of identified Software versions relative to Customer's current and future Software feature requirements.

Deliverables

- Type 3 Software Track Conformance Report
- Type 3 Software Analysis and Release Standards Report
- Note: One (1) quantity of Type 3 Software Analysis and Release Standards Report is for one (1) platform and its software release.

1.2.3c. Type 3 – Software Risk Management and Insights

Type 3 Software Risk Management and Insights consist of the following reports described below:

- Type 3 Product Security Advisory Customer Impact Assessment Report
- Type 3 Software Lifecycle Milestones Report

Technologies Supported

- Routing and Switching
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Software Defined Access
  - Routing and Switching
  - Security Policy and Access

Cisco Responsibilities

- Perform the following customer impact assessment when applicable for a published Cisco Product Security Advisory:
  - Identify list of devices affected or potentially.
- Provide analysis and recommendations to address how the Cisco Product Security Advisory may impact Customer's existing deployed Solution.
- Provide recommended Software version where the fix for the Cisco Product Security Advisory is incorporated.
- Assess devices affected by Software deferral, Software EOS, and Software EOL that are applicable to Customer's deployed Software standards and could result in a migration trigger.

Deliverables

- Type 3 Product Security Advisory Customer Impact Assessment Report
- Type 3 Software Lifecycle Milestones Report

1.3. Availability Insights

Availability Insights predicts device issues through near-real time and automated factor-based algorithms, correlated findings and recommendations for remediating issues to realize availability gains.

Availability Insights consists of the following features described below:

- Automated Fault Management
- Device Stability Factor

1.3.1. Automated Fault Management

Automated Fault Management analyzes device syslogs using Cisco rules and algorithms to detect Software, Hardware, and configuration faults in the Network, and deliver remediation instructions to the Customer. Historical trends and predictive algorithms can identify impending faults. Syslogs are monitored near-real time to detect sequences that indicate a fault has happened or is imminent. When detection occurs, the system may collect device data required for problem resolution, which may result in a notification and / or opening a case with Cisco support.

Technologies Supported

- Routing and Switching

Cisco Responsibilities

- Explain system deployment and operational requirements.

- Configure and deploy Automated Fault Management virtual machine (VM) in Customer's Network to process syslogs and open support cases.
- Inform Customer of one or more of the following when fault detection has occurred:
  - Notification of faults detected
  - Any collected data
  - Suggested remediation steps
  - Support cases
- Update managed device information on the Automated Fault Management server based on Customer-supplied information (as often as once per week).

Deliverables

- Quarterly Faults Detected and Service Request Status Report

Customer Responsibilities

- Provide specified deployment and runtime environment for Cisco Automated Fault Management Server VM.
- Provide Cisco Automated Fault Management Server with communications access to devices under Service for collection of configuration and status data.
- Provide Cisco Automated Fault Management Server with encrypted communications access to Cisco-hosted servers for the purpose of support case management and Software Updates to Automated Fault Management Software.
- Provide Cisco with device list and access credentials for all Network devices under Service, and update said list promptly when Network changes occur; this information may be supplied via API to Cisco Network Collector device, if present, or by formatted electronic record provided to Cisco personnel.
- Configure devices under Service to send syslog messages to a syslog server. Configure syslog server to forward the syslog events to Automated Fault Management VM.
- Provide access to email server for Automated Fault Management Server. Provide email addresses for notification emails.
- Integrate alarm management system with Cisco Automated Fault Management using Rest API, if desired; Cisco will not perform this work.

1.3.2. Device Stability Factors

Device Stability Factors collects near-real time information and assists Customer with recommendations for mitigating factors which affect the health and stability for top impacted devices.

Technologies Supported

- UCS Computing Systems

Cisco Responsibilities

- Device Stability Factor collects in near-real time stateful information and provides recommendations for mitigating stability risk for top impacted devices.
- The following insights are provided:
  - Overall compute infrastructure best practices health
  - Dynamic Identification, prioritization, and aggregation of component-level stability health scores and trends
  - Identification of anomalies and affected components.
  - Correlated findings and recommendations for improving stability of infrastructure.

Deliverables

- Compute data collected by Device Stability Factors and periodically reviewed by Cisco SME

Customer Responsibilities

- Provide specified deployment and runtime environment for Device Stability Factor Software. The Device Stability Factor data collection engine(s) are separate from CSPC.

- Provide Cisco with device list and access credentials for all devices supported by Device Stability Factor Software, and update said list promptly when changes occur.

1.4. Technology Assessments

Technology Assessments identify gaps and assist Customer with recommendations for optimizing the capacity, reliability, general performance, and/or security of Cisco technologies.

1.4.1. Resiliency Assessment

The Resiliency Assessment evaluates the resiliency and availability for enabling secure, reliable, high-quality Network and application services. The assessment focuses on resiliency and availability improvements to the architecture and operations of the Cisco technology.

Technologies Supported

- Routing and Switching
- Optical Networking
- Data Center Switching
-
-
-
-
- SP Video Infrastructure

Solutions Supported

- Software Defined WAN
  - Routing and Switching

Additional Information to be Collected

- Baseline of current availability and impact from service interruptions.

Cisco Responsibilities

- Provide recommend improvements, primarily focusing on availability and resiliency; improvements may include, but are not limited to:
  - Design and configuration changes.
  - Monitoring features.
- Provide a roadmap and an agreed-upon priority for resiliency improvements.

Deliverables

- Resiliency Assessment Report

Limitations

The following limitations are specific only to the technology listed.

- **Routing and Switching:**
  - Resiliency Assessment covers only Cisco Routing and Switching networking devices (up to 5000 Cisco devices).
  - Cisco Wi-Fi Hardware and Software lifecycles along with manageability and security best practices are included in the analysis. Wi-Fi specific configurations and Radio Frequency (RF) studies are not covered in the Routing and Switching Resiliency Assessment; these activities are supported within the WLAN RF Assessment Deliverables.
  - Cisco Firewall and load-balancer Hardware and Software lifecycles are included in the analysis, but Firewall and load-balancer rules are not included.
  - VoIP configurations are out-of-scope.
  - Third-party equipment is out-of-scope.
  - Resiliency Assessment analyzes and makes recommendations addressing the existing Network infrastructure and does not make recommendations based on future Network designs.
  - Resiliency Assessment does not offer any Network performance analysis, application analysis, or Network bandwidth utilization assessments.

- **SP Video Infrastructure:**
  - Resiliency Assessment performed for SP Video Infrastructure will focus on End-User Availability Assessment, and does not assess the entire Network availability.
- **Optical Networking:**
  - One (1) Resiliency Assessment Report supports a maximum of fifty (50) devices.
  - The scope of the Resiliency Assessment will focus on protection schemes and alternate routing at the hardware level only. Resiliency of power plant, circuit and node capacity, and third-party products is out of scope.

1.4.2. Network Device Security Assessment

Network Device Security Assessment assists Customer with analyzing device configurations to help identify security gaps and provide recommendations to remediate gaps in the configurations.

Technologies Supported

- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat

Additional Information to be Collected

- Customer's device security templates, device configurations, and policies.

Cisco Responsibilities

- Review Customer's device security goals and requirements.
- Assess up to 350 Cisco device configurations; only ten (10) of those devices may be firewalls. A maximum of two (2) FTD clusters.
- Analyze device configurations, focusing on configuration security hardening of the individual devices.
- Analyze firewall rules for common configuration issues.

Deliverables

- Network Device Security Assessment Report

Limitations

The following are the supported OS types for Network Device Security Assessment:

- Supported Operating Systems:
  - Cisco IOS
  - Cisco IOS XR
  - Cisco NX-OS
  - Cisco IOS-XE
  - Cisco ASA / ASASM
  - Cisco FWSM
  - Cisco PIX
  - Cisco FTD
  - Cisco WSA
  - Cisco CAT-OS

1.4.3. Collaboration Security Assessment

Collaboration Security Assessment provides Customer with a Security Assessment Report, recommendations, and risk analysis of five critical Solution elements:

- **Collaboration Network Infrastructure**: Network Segmentation / VLANs, quality of service, Access Control Lists, Hardware and Software, DHCP, DNS, TFTP, and NTP.

- **ID & Access Management:** access privilege, account management, access logging, configuration change management
- **Call Control**: Cisco Unified Communications Manager (CUCM), Voice gateways, SIP trunks, Cisco Unified Border Element (CUBE), dial plan, signaling, and media.
- **Endpoints**: Cisco Unified IP phones, soft phones, Video endpoints, and devices that connect to the IP Network.
- **Applications**: User applications such as CUCM, Unified Messaging, Conferencing, Video, Customer Care, and custom tools extend the capabilities of IP communications systems.

Architecture Supported

- Collaboration

Additional Information to be Collected

**Specific to Collaboration Security*

- UC infrastructure, which may include the following:
  - Historical CUCM call detail records
  - Dial-plan report and log(s) report
  - Analysis of CUCM call routing
  - Media and signaling protection
  - Endpoints
  - Applications
  - Voice Gateway, SIP Trunk / CUBE data
- Customer Care infrastructure, which may include the following:
  - Windows Operating System (OS) Server
  - MS SQL Server
  - Windows Firewall / Ports
  - Anti-virus
  - Remote Desktop
- Video Collaboration infrastructure, which may include the following:
  - Video applications
  - Call control
  - Conferencing
  - Video endpoints
- Collaboration edge

Cisco Responsibilities

The scope of the Collaboration Security Assessment will focus on one or both of the following areas specified in the Quote:

- Toll Fraud
- Telephony Denial of Service (TDoS)

Customer Requirements Validation

- Verify Customer's selected Collaboration Solution endpoints and security concerns.
- Confirm application servers and hosting location, along with Customer security concerns.
- Validate Collaboration Solution deployment model (physical and logical) and security requirements (if any).
- Verify any federated connections or business-to-business applications running in the Network.
- Verify PSTN (SIP) trunking and security applied, as applicable.

Security Assessment

- Assess the effectiveness of Network security controls intended to protect the Customer Collaboration Solution.
- Perform Software risk analysis on Collaboration application servers and endpoints.
- Analyze and compare Customer security policies with Cisco leading Collaboration security best practices.

- Conduct analyses on CUCM and voice gateways or SIP trunks, as applicable.

Deliverables

- Collaboration Security Assessment Report
- Collaboration Security Assessment Executive Summary

Customer Responsibilities

- No major changes are made to the Collaboration infrastructure while the Security Assessment is in progress, which may take up to four (4) weeks depending on the complexity of the environment.

1.4.4. Radio Frequency Verification Assessment

The Radio Frequency (RF) Verification Assessment surveys the RF environment and provides an analysis and recommendations for optimal RF performance and coverage.

Technologies Supported

- Wireless Networking

Additional Information to be Collected

- Measurements of internal / external interference at one moment in time.

Cisco Responsibilities

- Validate RF performance and coverage of the WLAN against the documented WLAN design.
- Survey the RF environment for coverage, interference, general performance, and Network configuration.

Deliverables

- RF Verification Document

1.4.5. WLAN Radio Frequency Assessment

WLAN RF Assessment works to identify RF signal propagation for optimizing wireless access point (AP) placement. Cisco performs an On Site survey to capture and evaluate site details, including physical and environmental considerations, electrical and AC / DC supplies, cabling, Network synchronization, peripheral equipment, and remote access.

Technologies Supported

- Wireless Networking

Cisco Responsibilities

- Conduct an On Site survey of the RF environment for coverage, interference, general performance, and Network configuration.
- Perform critical RF survey to determine the optimal AP placement.
- Develop recommendations for site modification and improvements by performing analyses that include:
    - RF Coverage Analysis.
    - Interference Analysis.
    - RF Spectrum Analysis (Optional).

Deliverables

- Site Survey Report

2. OPERATIONAL PROFICIENCY

Operational Proficiency assists Customer with recommended improvements to the maturity of operational process, measurement, tooling capabilities, and resources that help increase skills and knowledge of Cisco technologies.

SECTION NAVIGATION

Operational Proficiency includes the following Service capabilities and Deliverables:

2.1. Instrumentation Management

Instrumentation Management assists Customer with analysis of management goals against current capabilities and features, assesses impact of new requirements, and recommendations to align management Solution design with priorities, goals, and objectives.

2.1.1. Management Instrumentation Review

Management Instrumentation Review assists Customer's operations staff to achieve current and future Network Management business and operational objectives by incorporating Cisco's architecture and operational best practices.

Cisco Engineers assess Customer's Solution architecture and technical design requirements (capability, resiliency, efficiency, scaling), perform a current-state capability and risk assessment, and recommendations to help Customer achieve business and operational objectives. Cisco optimizes visibility and control of Customer's IT environment for one (1) architecture.

Technologies Supported

- Network Management and Orchestration

Solutions Supported

- Software Defined WAN
  - Network Management and Orchestration

Cisco Responsibilities

- Focus Services on areas that may include Event Management, Incident Management, Problem Management, Change Management, Service Management, Asset and Configuration Management, IT Service Catalog Management, Performance and Capacity Management, Security Management, Knowledge Management, Automation / Orchestration, and Billing and Chargeback.
- Analyze Customer's requirements, current practices, and capabilities compared to Cisco-recommended best practices.
- Analyze impact of new requirements on existing Network Management infrastructure and operations support.
- Provide assistance in aligning Management Instrumentation design with Network architecture evolution.
- Update current Network Management Instrumentation design Documentation.

Additional Responsibilities

**Specific to Network Management and Orchestration*

- Review and provide recommendations for the following:
  - Management protocol selection and configuration
  - Feature selection and configuration of existing Network Management Instrumentation applications
  - Security considerations

Deliverables

- Management Instrumentation Review Report

2.1.2. Management Deployment Planning and Readiness Assessment

The Management Deployment Planning and Readiness Assessment Service assists Customer's Operations staff to prepare for management Software Solution post-implementation maintenance. Cisco validates Customer implementation plans and processes, reviews test cases and results, and advises on impact to operational processes.

Technologies Supported

- Network Management and Orchestration
- Packet Core
- Data Center Orchestration and Automation

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
- Software Defined WAN
  - Network Management and Orchestration
- Software Defined Access
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)

- Computing Systems
- Data Center Switching
- Data Center Orchestration and Automation
- Packet Core

- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

Cisco Responsibilities

- Validate Customer Solution implementation plans and processes.
- Validate Customer Solution test objectives, plans, results, and issues.
- Advise Customer on recommended improvements to address operational process capabilities and readiness.

Deliverables

- Consultative guidance and support only

2.2. Metrics Management

Metrics Management assists with reviewing measurement goals and requirements; evaluates effectiveness of current metrics against recommended metrics and tooling capabilities; and helps with steps to define, align, measure, and report on KPIs to improve visibility and decision-making.

2.2.1. KPI Definition, Implementation, and Report

The KPI Definition, Implementation, and Report Service provides assistance to define and establish a framework for measuring Cisco Management Software Solution and system Critical Success Factors (CSF) and KPIs. The scope of KPIs can include functional KPIs, such as Service provisioning, fault, performance, and configuration management, as well as system performance KPIs including memory, processing, and database capacity.

Technologies Supported

- Network Management and Orchestration
- Data Center Orchestration and Automation

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Software Defined Access
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration

Exclusion

**Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

Cisco Responsibilities

- Evaluate potential Customer-required KPIs based on Cisco-recommended KPIs.
- Define KPI data collection sources, process, automation opportunities, and target thresholds.
- Define KPI functional ownership, process ownership, and review frequency.

Deliverables

- KPI Framework Report

Customer Responsibilities

- Provide CSF and KPI requirements and priorities.

2.2.2. KPI Audit and Recommendation

KPI Audit and Recommendation collects and analyzes KPIs from the Cisco Solution over a specified timeframe, and looks for issues in the areas of Fault, Performance, Capacity, and Configuration Management that relate directly to the stability and availability of Customer's Solution. Quote for Services will specify the Cisco Solution(s) supported.

Technologies Supported

- Mobility Policy and Access
- Packet Core

Solutions Supported

- Cisco Policy Solution (CPS),
- Self-Optimizing Network (SON)
  - Mobility Policy and Access
- Software Defined Access
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration

Cisco Responsibilities

- Create the KPI Audit and Recommendations Report:
- For Cisco Policy Solution (CPS):
  - If applicable, the following KPIs on both Gx and Gy interface will be part of the report:
    - Credit Control Request – Success, dropped, and error rate.
    - Reauthorization request – Success, dropped, and authorization rate.
    - If applicable, the following KPIs on Sy interface will be part of the report:
      - Spending Limit Request – Success rate.
      - Spending Status Notification – Success rate.
      - Session Termination Request – Success rate.
- For Cisco SON Solution:
  - Top Offender Analysis and Recommendations:
    - Generate monthly reports for top offenders with highest drop-call rate (DCR).
    - Optimize SON settings for these offenders to get KPI improvements.
    - Recommend preliminary Solutions for top offenders.
  - SON Reports: KPI / Boomer Report:
    - Boomer and Primary Scrambling Code (PSC) collision reports will be provided based on Customer's request.
    - Activity Report for application to show SON actions.
    - KPI metrics for Remote Network Controllers (RNC) and Network level.
    - Count of new cell neighbor activity by SON.
- For Cisco Prime® Access Registrar:
  - If applicable, the following will be part of the report:
    - Systems KPIs
    - Defined Counters
    - Radius Counters
    - Rest KPIs

Deliverables:

- KPI Audit and Recommendations Report

2.2.3. KPI Trending and Reporting

KPI Trending and Reporting assists Customer with recommended improvements to Cisco Management Software Solution, process, system KPIs trends and deviations from the baseline. Scheduled Service is performed at a frequency agreed with the Customer (recommended once every quarter).

Technologies Supported

- Network Management and Orchestration
- Data Center Orchestration and Automation

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Software Defined Access
  - Network Management and Orchestration
- SP Analytics and Assurance
  - Network Management and Orchestration

Exclusion

**Specific to Data Center Orchestration and Automation*

- Cisco CloudCenter (CCC) is not supported.

Cisco Responsibilities

- Analyze Customer KPI performance trends to identify deviations from baseline targets.
- Evaluate multiple viewpoints such as design, capacity, support, and operations.

Deliverables

- KPI Evaluation Report

2.2.4. Security Metrics Program Development

Cisco will assist Customer in developing a Security Metrics Program, including analysis and creation of an initial security metrics catalog and dashboards based on Customer needs and requirements.

Cisco will leverage recognized standards for security measurement and metrics, including ISO 27004: Information Technology – Security Techniques – Information Security Management – Measurement. Cisco uses a combination of approaches to deliver a Security Metrics Program Development engagement, including educational workshops, individual and group working sessions, and review of artifacts. The resulting Deliverables will include recommendations for strategic and tactical improvement of the measurement program, as well as specific metrics and dashboards developed over the course of delivery.

Architecture Supported

- Security

Cisco Responsibilities

- Review the maturity of the Customer's current IT and Information Security Measurement Program.
- Facilitate an introductory Security Metrics Workshop with business and technical resources to:
- Provide an overview of measurement in industry.
- Provide an overview of specific measurement applications in information and IT security.
- Provide an overview of ISO 27004 and other appropriate security measurement standards and frameworks.
- Explain the Goal-Question-Metric (GQM) methodology.
- Discuss specific security measurement examples and case studies.
- Discuss and identify key security questions and metrics that need to be answered and reported on a regular basis.

- Analyze workshop results and applicability to the overall engagement.
- Compare existing program to recommendations and requirements of ISO 27004 and other measurement frameworks.
- Facilitate GQM workshops with business and technical resources for purposes of developing and improving the Customer's metrics catalog, which may include the following activities:
- Use GQM techniques to define and explore specific strategic measurement scenarios for new or existing Customer security metrics.
- Analyze GQM results and incorporate them into the metrics catalog.
- Provide recommendations for executive and management dashboards as well as a roadmap for metrics maturity.

Deliverables

- Security Metrics Recommendation Report

2.3. Operations Management

Operations Management assists Customer with steps to evaluate and remediate risk of operational gaps. Cisco and Customer will collaborate with Cisco Technical Assistance Center (TAC) and appropriate business units for open Cisco Priority 1 (P1) and Priority 2 (P2) cases.

2.3.1. Escalation Engineering Support

Escalation Engineering Support enhances the Customer's Incident and Problem Management process by providing assistance with Cisco TAC restoration of Service activities for unplanned or unscheduled incidents.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Data Center Orchestration and Automation
- Tetration
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Next Gen Cable Access
- IoT Edge and Fog Compute

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Packet Core
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security
- Managed Services Accelerator (MSX)
  - Routing and Switching

- Network Management and Orchestration
- Computing Systems

Cisco Responsibilities

- Perform technical evaluation with Cisco TAC escalation after following the proper Cisco TAC procedures, diagnosis, and escalation process.
- Collaborate with Cisco TAC regarding Customer's Cisco environment to assist Cisco TAC and the appropriate Cisco business unit(s) in resolving the incident.
- Assist Customer with Remote support in dealing with open P1 and P2 cases.
- Assist Customer in analyzing recurring problem(s) and root cause(s), including providing consultative support for development of a plan of action to prevent, address, and minimize the business impact of the problem(s).

Additional Responsibilities

**Specific to Unified Communications, Customer Care, Video Collaboration, Cloud Meetings and Messaging*

- Cisco Project Manager will assign an Engineer to remotely track and help with the reSolution of the issue(s) related to the Cisco Collaboration Solution for P1 and P2 cases only.

Deliverables

- Consultative guidance and support only

Customer Responsibilities

- Provide Cisco access to users that have been contacting the Customer's support desk or reSolution center for assistance in connection with the Cisco components or Service problems or issues.
- Notify Cisco Services of the open ticket needing assistance, and provide Cisco TAC case number.

Note: Customer shall not escalate any related problems or issues until Cisco TAC has performed diagnostics.

- Work with Cisco TAC on the resolution and closure of problem / case, and involve Cisco Network Consulting Engineer only on critical P1 and P2 cases, as needed.

Limitations

- The following are not provided or a part of the Escalation Engineering Support Service:
- Cisco Services Engineer does not make any changes to the Customer Production environment.
- The Service does not cover P3 / P4 Cisco TAC cases.
- There must be an onsite presence for Cisco TAC case support.
- This Deliverables does not replace Cisco TAC, Cisco High-Touch Operations Management, Cisco High-Touch Technical Support, or any other form of technical Services and support, including Third-Party Support.
- Cisco Technical Services, Cisco TAC, and any of the following Services Customer may have, such as High-Touch Technical Support, High-Touch Operations Management, and Focal Engineer, are responsible for case escalation, resolution, and engaging and involving appropriate resources like Cisco business unit(s) and third-party vendors, as well as for providing any and all status updates and communications related to the case and case closure.

2.3.2. Asset Management

Asset Management assists Customer with recommended Cisco best practices for managing assets and contracts based on the Customer inventory, reporting of asset moves, adds, changes and deletions (MACD), and monitoring of asset coverage and entitlement.

Asset Management has two levels:

- Standard

- Premium

Premium Level Asset Management provides a higher engagement and customization level than the Standard Level.

Solutions Supported

- Expert Care

Additional Information to be Collected

- Customer's record of inventory and service contract details.
- Customer's record of serial number removed and replaced by Return Material Authorization (RMAs).

Cisco Responsibilities

- Provide the following common responsibilities:
- Provide reporting on the Customer's inventory which may include the following:
  - Changes to address inventory Service coverage, co-termination, and location.
- Provide documented process for IT asset moves, adds, changes and deletions.
- Provide the following Asset Management Standard or Premium Level as specified on the Quote:

• Asset Management	• Standard Level	• Premium Level
Customer Engagement Level		
1.1 Resource Allocation	• Designated	• Designated
Resource Location	• Remote	• Remote
On-Site Visits	• Not Applicable	• 4 times per year
2.0 Establish and Maintain Consolidated Install Base (IB)		
2.1 Business Entity Resource and Qualification	• Supported	• Supported
2.2 Establish and Maintain IB Baseline	• Supported	• Supported
2.3 Frequency of IB Updates	• Monthly	• Monthly
3.0 Reconciliation / Clean-Up		
3.1 Identify and Fix Data Discrepancies	• Supported	• Supported
4.0 Reporting Analysis and Business Review		
4.1 Reporting IB Baseline	• Supported	• Supported
4.2 Business Reviews	• 2 times per year, remote	• 4 times per year, on site
4.3 Reporting and Analytics	• Standard	• Customized
4.4 Business Review and Consulting	• Standard	• Customized

Deliverables

- Deliverables provided are based on the Asset Management Standard or Asset Management Premium Level of Service as specified in the Quote.

Customer Responsibilities

- Designate a representative to act as the primary interface for Asset Management; this representative will work with Cisco's Asset Manager to resolve any issues related to Asset Management

2.3.3. Incident Management

Incident Management provides a single point of contact, a Cisco High-Touch Operations Manager ("HTOM"), for the management of all incidents. The HTOM has knowledge of the Customer processes, Cisco support organizations, escalation process and coordinates to help restore Customer service operations. For Onsite Incident Management this Deliverables must be purchased with Operations Onsite Support Deliverables.

Note: Service Monitoring and Reporting Deliverables is provided with Incident Management.

Solutions Supported

- Expert Care

Additional Information to be Collected

- Customer's Network Operations Center (NOC) setup such as staffing groups, tools, communications and escalation process, contacts, field support groups.

Cisco Responsibilities

- Facilitate problem resolution on a reactive basis for technical issues reported to Cisco by Customer.
- Provide twenty-four (24) hours a day, seven (7) days a week incident management for case request and escalation management support for Severity 1 and Severity 2 cases during non-Standard Business Hours.
- Follow-ups within Cisco and Customer, and identify Service Request response gaps.
- Coordinate Cisco support organizations, escalation process, and Customer resources for Service Requests.
- Conduct post incident review to determine recommendations for corrective actions and best practices for improving operational support processes.
- Conduct operational assessment of Customer's current processes and recommend best practices for incident and event management.

Deliverables

- Facilitate incident and problem resolution

2.3.4. Service Monitoring and Reporting

Service Monitoring and Reporting assists the Customer with recommended operations best practices, data-driven insights and KPIs related to incidents for improvements to service quality, service performance and operational efficiency gains.

Dependency

- Service Monitoring and Reporting requires purchase of Incident Management Deliverables.
- Reporting of Root Cause Analysis and Recommendations requires purchase of Problem Management Deliverables.

Solutions Supported

- Expert Care

Additional Information to be Collected

- Established processes and procedures used for support.

Cisco Responsibilities

- Provide status and reporting, escalation assistance, and coordinate the return of parts requiring Engineering Field Analysis ("EFA").
- Review status and progress of Service Delivery levels, open Service Requests, follow-up on actions and address outstanding issues.
- Conduct a quarterly review of Deliverables and activities provided during the immediate past timeframe and actions planned for the next quarter.
- Conduct regular proactive operations excellence assessments.
- Create Customer profile for Cisco Technical Services knowledge of Customer's operations processes, procedures, and network access for support.
- Provide Service Incident Reporting which may include the following as applicable:

- Cisco Service Requests, Known Errors, Post Incident Operational Improvements, Root Cause Analysis and Recommendations, Operational Abnormalities and Trends.
- KPI and Analytics reporting focused on analytics to improve operational efficiency

Deliverables

- EFA Coordination and Reporting
- Service Delivery Level Reporting
- Incident Management Readiness Assessment
- Service Incident Reporting
- Analytics and KPI Dashboard Reports

2.3.5. Problem Management

Problem Management provides access to Cisco High-Touch Technical Support or Cisco High-Touch Engineering familiar with your networking environment.

2.3.5a. Problem Management - High-Touch Technical Support

Provides twenty-four (24) hours a day, seven (7) days a week direct access to a Cisco High-Touch Technical Support ("HTTS") team of specialists. The HTTS team helps troubleshoot your Cisco network for complex and critical issues and provides remediation support to help resolve identified issues. HTTS provides two support options: a pooled High-Touch Technical Support team, or Dedicated High-Touch Technical Support team.

Dependency

- Incident Management Service is required.

Additional Information to be Collected

- Customer's proposed current and planned hardware changes, software upgrades and or configuration changes, methods of procedures (MOP).

Solutions Supported

- Expert Care

Cisco Responsibilities

- Provide case tracking and troubleshooting which includes the following:
- Provide direct access where available, twenty-four (24) hours per day, seven (7) days per week basis to a HTTS team via a Cisco provided contact information.
- Provide proactive maintenance window support which includes the following:
- Work with the Customer to create a Service Request for a scheduled maintenance window.
- Provide recommended changes to Customer's implementation plan, MOP, and test plan based on information gathered from the Customer.
- Provide remote standby support during scheduled maintenance window.

Note: The Cisco Expert Care Service Level Agreement terms and conditions for Response Time and Restoration Time is documented in the Cisco Business Critical Services General Terms Section 5 - Cisco Expert Care Service Level Agreement.

Limitations

- Cisco is not responsible for testing any procedures in support of Customer's proposed or planned changes.
- Cisco is not responsible for developing MOPs.

Deliverables

- Case Tracking and Troubleshooting

- Proactive Maintenance Window Support

Note: The Quote will specify pooled or dedicated High-Touch Technical Support.

2.3.5b. Problem Management - High-Touch Engineering

Provides direct access to a Cisco High-Touch Engineer (HTE), which has both technical knowledge and familiarity with your networking environment. The HTE helps troubleshoot your Cisco network for complex and critical issues and provides remediation support to help resolve identified issues. For Onsite Problem Management – High Touch Engineering this Deliverables must be purchased with Operations Onsite Support Service.

Dependency

- Incident Management Deliverables are required with this Service.
- Performance of a root cause analysis by Cisco is dependent upon all the necessary information available to Cisco in a timely manner.

Additional Information to be Collected

- Customer's proposed current and planned hardware changes, software upgrades and or configuration changes, methods of procedures (MOP).

Solutions Supported

- Expert Care

Cisco Responsibilities

- Provide case tracking and troubleshooting which includes the following:
- Provide direct access where available, during Standard Business Hours, to the HTE via a Cisco provided contact information.
- Perform root cause analysis on high severity technical issues in the Network Infrastructure.
- Provide proactive maintenance window support which includes the following:
- Work with the Customer to create a Service Request for a scheduled maintenance window.
- Provide recommended changes to Customer's implementation plan, MOP, and test plan based on information gathered from the Customer.
- Provide remote standby support during scheduled maintenance window.

Deliverables

- Root Cause Analysis Report
- Problem Management
- Proactive Maintenance Window Support

2.3.6. Self-Optimized Network (SON) Scheduled Event / Venue Support

SON Scheduled Event / Venue Support provides proactive support to prepare for large-scale scheduled Customer events (games or conferences) that utilize Customer's Radio Access Network (RAN) resources. Cisco provides assistance to plan, implement, and support major SON application module configurations.

Solutions Supported

- Self-Optimizing Network
  - Mobility Policy and Access

Additional Information to be Collected

- Business and technical requirements for Mass Event Handling (MEH) application module configuration.
- Scheduled Customer Event / Venue details

Cisco Responsibilities

- Assist Customer to configure MEH application modules to meet Customer event and venue networking requirements.
- Provide proactive support for Network freeze / rehome and any other major scheduled Radio Access Network (RAN) activities for SON.
- Review Customer RAN reports of anticipated network load or traffic.

Deliverables

- Consultative guidance and support only

2.4. Knowledge Management

Knowledge Management assists Customer efforts to enhance technical knowledge and operational skills with Knowledge Transfer Sessions for Operations, access to Cisco Technical Knowledge Library, Cisco training, and specialized technical training workshops.

2.4.1. Knowledge Transfer Session for Operations

Knowledge Transfer Session for Operations provides technical information transfer on topics mutually agreeable and relevant to the Cisco Products and technologies deployed in Customer's environment. Sessions focus on best practices for operating, tuning, troubleshooting, maintaining, and managing Cisco Solutions deployed. Knowledge transfers are not formal trainings or replacement for any authorized Cisco Education classes.

Technologies Supported

- Routing and Switching
- Optical Networking
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Tetration
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Hosted Collaboration Solution
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- Next Gen Cable Access
- SP Video Infrastructure
- IoT Edge and Fog Compute
- Industrial Networking and Collaboration

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Virtual Packet Core
  - Packet Core
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Software Defined Access
  - Routing and Switching
  - Wireless Networking
  - Network Management and Orchestration

- Computing Systems
- Data Center Switching
- Data Center Orchestration and Automation
- Packet Core

- Managed Services Accelerator (MSX)
  - Routing and Switching
  - Network Management and Orchestration
  - Computing Systems
  - Security Policy and Access
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

Cisco Responsibilities

- Consult with Customer to identify requirements and topics for Knowledge Transfer Sessions at least forty-five (45) days in advance; Knowledge Transfer Sessions are:
  - Relevant to the Cisco Products and technologies deployed in Customer's Production Network.
  - Delivered by Cisco Services Engineer remotely using virtual web conferencing for up to four (4) hours in length with no labs and no printed course materials.
  - Delivered based on a specific number of sessions as specified in the Customer Quote.

Additional Responsibilities

**Specific to Unified Communications, Video Collaboration, Customer Care, Cloud Meetings and Messaging*

- Record all Knowledge Transfer Sessions.
- Share session recordings with Customer for future reference.

**Specific to Packet Core*

- For Cisco Virtual Packet Core, this deliverable supports RedHat OpenStack and RedHat Operating System software components.

Deliverables

- Knowledge Transfer Session Slides, if applicable.

Customer Responsibilities

- Coordinate and schedule Knowledge Transfer Sessions with a Cisco Project Manager at the beginning of each quarter.
- Provide attendees familiar with Cisco Products related to the Customer's Solution.
- Provide a maximum number of attendees at any one time that shall not exceed ten (10), unless mutually agreed upon by the Customer and Cisco.

Limitations

**Specific to Hosted Collaboration Solution*

- For the HCS Standard Service: Knowledge Transfer Sessions will be limited to two (2) sessions.
- For the HCS Premium Service: Knowledge Transfer Sessions will be limited to four (4) sessions.

2.4.2. Learning Library

Learning Library provides access to Cisco Services leading best practices, case studies, books from Cisco press, on-demand technical assets, on-line courses and interactive hands-on labs.

The following two libraries are available:

- Technical Knowledge Library
- Platinum Learning Library

2.4.2a. Technical Knowledge Library

Technical Knowledge Library (TKL) is a subscription-based Service that provides access to Cisco Services best practices and technical knowledge developed by Cisco Services Engineers. The library provides end-users with access to learning resources and technical information such as whitepapers, design and implementation guides, case studies, books from Cisco press, live webinars, and videos-on-demand. The library is made available by Cisco through a secure, web-based portal.

TKL is only available to certain geographic locations and will be specified in the Quote.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Unified Communications
- Customer Care
- Video Collaboration
- Cloud Meetings and Messaging
- Hosted Collaboration Solution
- Network Security
- Cloud Security
- Security Policy and Access
- Advanced Threat
- Packet Core
- Mobility Policy and Access

Solutions Supported

- Virtual Packet Core
  - Packet Core

Cisco Responsibilities

- Make content available to the specified number of authorized viewers in the Customer's Quote, including multimedia clips in the form of video-on-demand or audio-on-demand content, as well as sidebar content such as whitepapers, case studies, design guides, configuration guides, troubleshooting guides, training documents, deployment guides, online textbooks and/or manuals, or bumper clips.
- Provide list of web-based trainings delivered via the portal to authorized viewers.

Note: Cisco may revise, Update, and/or remove previously released multimedia clips and/or sidebar content (Updated Content). Cisco will make any Updated Content available to Customer as a part of the Services. The Updated Content will exclude the previously released multimedia clips and sidebar content (where applicable) that the Updated Content was intended to supersede.

Deliverables

- Access to TKL, an online library of learning resources and technical information

2.4.2b. Cisco Platinum Learning Library

The Cisco Platinum Learning Library (CPLL) consists of a collection of on-demand technical assets, on-line courses and interactive hands-on labs. A Cisco Learning Advisor assists the Customer with curriculum recommendations and CPLL course consumption.

Solutions Supported

- Expert Care

Cisco Responsibilities

- Access to a Cisco Learning Advisor to assist with curriculum recommendations and CPLL course consumption
- Provide access to CPLL on-demand technical assets, on-line courses and interactive hands-on labs.

Deliverables

- Access to Cisco Platinum Learning Library

Note: Number of seats to access the CPLL will be specified in the quote.

2.4.3. Cisco Training

- Cisco Training provides access to a catalog of more than 250 different courses on certification and product training available for open and closed (private group) enrollment. A Cisco Learning Advisor assists the Customer with course selection and scheduling.

2.4.3a. Cisco Open Enrollment Training

Cisco Open Enrollment Training provides access to a catalog of instructor-led certification and product training courses, available for open enrollment to the public. Training is delivered at Cisco training facilities or at Cisco Authorized Learning Partners. A Cisco Learning Advisor assists the Customer with course selection and scheduling.

Solutions Supported

- Expert Care

Cisco Responsibilities

- Seats in publicly offered classes from a catalog of instructor-led certification and product training courses. Classes are delivered live or virtually.

Deliverables

- Seats in Cisco Open Enrollment Training

Customer Responsibilities

- At least forty-five (45) days in advance of a course provide a list of participants, their role and function as it relates to the focus of the course.
- Coordinate and schedule Cisco Training with a Cisco Learning Advisor.

2.4.3b. Cisco Closed Enrollment Private Group Training

Cisco Closed Enrollment Private Group Training provides access to a catalog of instructor-led certification and product training courses, available for a private group of up to twelve (12) people. Training is delivered at the Customer's location and tailored to their network. A Cisco Learning Advisor assists the Customer with course selection and scheduling.

Solutions Supported

- Expert Care

Cisco Responsibilities

- Seats in private group training classes from a catalog of instructor-led certification and product training courses. Classes are delivered live or virtually.

Deliverables

- Seats in Cisco Closed Enrollment Private Group Training

Customer Responsibilities

- At least forty-five (45) days in advance of a course provide a list of participants, their role and function as it relates to the focus of the course.
- Coordinate and schedule Cisco Training with a Cisco Learning Advisor.

2.5. Classified Network (U.S. Only)

Classified Network provides Deliverables which assist the Customer with Services for supporting Classified Network.

2.5.1. Classified Network Support

Cisco Classified Network Support (CNS) assists the Customer with facilitating timely problem reSolution of issues reported to Cisco. Customers are provided reactive, direct, around the clock support by cleared support engineers familiar with Customer's Network design and operations. CNS delivers advanced technical troubleshooting using a pool of certified experts on a wide variety of technologies and Cisco Solutions.

Classified Network Support consists of the following components:

- CNS High-Touch Operations Management
- CNS High-Touch Technical Support

2.5.1a. CNS High-Touch Operations Management (U.S. Only)

Note: CNS High-Touch Operations Management Deliverables is purchased using a single Cisco Business Critical Services SKU CON-AS-RS-OPT which assists the Customer with issues reported for any of the technologies listed below.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Unified Communications
- Video Collaboration
- Network Security
- Security Policy and Access

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Software Defined WAN
  - Network Management and Orchestration
  - Routing and Switching

Cisco Responsibilities

- Designate a Cisco Classified Network Support person (CNS Operations Manager) to act as the primary non-technical liaison point-of-contact to provide Deliverables and activities.
- Provide the following:
  - Case Request Escalation Management: Operations Manager will facilitate problem resolution on a reactive basis for technical issues reported to Cisco by Customer, and help Customer determine if appropriate resources are being applied to technical issues reported. This includes notifying Cisco TAC and the Cisco Engineer familiar with Customer's Network of any planned event by pre-opening case and alerting Cisco TAC of relevant information related to the scheduled event.
  - Base Reporting Package: Operations Manager will provide standard weekly, monthly, and quarterly reporting to Customer.
  - Quarterly Operations Data Analysis: Operations Manager will conduct quarterly discussion with Customer on Deliverables and activities to review alignment with Customer business objectives. This can include reactive

support contract usage, case statistics, quality issues, overall case analysis (such as Product type or case priority), Network analysis, and Return Materials Authorization (RMA) trending.
    - Extended Operational Analysis of Critical Issues: Cisco will perform operational data analysis, on critical issues by identifying Customer knowledge gaps and operational abnormalities / gaps. Cisco will provide recommendation and identify possible Solutions that Customer may elect to implement to help close knowledge and system quality gaps.
- Provide access to the Classified Network Support team via a Cisco-provided phone number for the following:
    - Provide case-tracking and troubleshooting where available, on an up-to twenty-four (24) hours-per-day, seven (7)-days-per-week basis as follows:
        - Severity 1 or Severity 2 calls: Response objective is within fifteen (15) minutes;
        - Severity 3 and Severity 4 calls: Response objective is within sixty (60) minutes during Standard Business Hours as extended therein to 8:00 am – 5:00 pm US Eastern Standard Time.
- Provide a Customer Portal for Incident Tickets:
    - Classify each incident ticket based on a modified version of the US-CERT incident categories: http://www.us-cert.gov/governmentusers/reporting-requirements.
    - Prioritize all Incidents, based on information known to Cisco at the time of incident creation, into High, Medium, and Low priority based on one or more criteria such as the type of infection, confirmation of the incident, or the number assets associated with the Incident. Priorities are defined as:
        - High: Critical business impact or data loss to the Customer
        - Medium: Adverse effect to Customer, potential data loss, potential loss of service.
        - Low: Minimal adverse impact to Customer. No financial loss. No data loss.
- Electronically notify designated Customer contacts for new incidents.
- Communicate mitigation recommendations if available for associated incident.
- Note any corrective actions requiring action by the Customer including gaps in the information provided.

Additional Responsibilities

*Specifically applies only if Customer has purchased this Deliverables in conjunction with Cisco Remote Managed Services

- Designate a CNS Operations Manager to act as the focal point for change management procedures.
- Define the high-level scope of work required to transition Customer's existing Network to readiness for management of the Managed Components by Cisco, including assessing changes required to Customer's platform, Network and processes in order to commence the Services.
- Provide and help manage a Transition Plan that defines the overall Service transition scope, establishes milestones against which project progress will be measured, defines the requirements for establishing connectivity and access for the Service, and establishes a go-live date (or set of dates) when Cisco will begin to managed and/or monitor the Managed Components.
- Define the required inventory information and topology requirements necessary to activate or onboard the Managed Components.

Deliverables

- Case Request Escalation Management
- Base Reporting Package
- Quarterly Operations Data Analysis
- Operational Analysis of Critical Issues
- Case Tracking and Troubleshooting
- Transition Plan (this Deliverables only applies if Customer has purchased Cisco Remote Managed Services)

Optional Deliverables Bundle

With the above Deliverables, the following Optional Deliverables bundle may be added. Deliverables and activities described below are available individually, in a grouping of two optional Deliverables or in its entirety. Customer may not select greater than two optional Deliverables unless all of the optional Deliverables bundles have been selected.

- Engineering Field Analysis (EFA) Coordination and Reporting: Coordinate the return of parts requiring a failure analysis and communication on the status to the Customer; regular reporting, status, and escalation assistance will be provided.
- Service Delivery Level Reporting: Provide reporting focusing on delivered Service levels.
- Custom Reports: Provide custom reports in support of either service level agreement (SLA) reporting requirements or as specified by the Customer.
- Onsite CNS Operations Manager: Provide a dedicated individual to perform Operations Management-related tasks at the Customer identified site for duration as specified in the Quote for Services.

Optional Deliverables Bundle

- EFA Coordination and Reporting
- Service Delivery Level Reporting
- Custom Reports
- Onsite CNS Operations Manager

Limitations

- For Case Request Escalation Management, pre-opening cases for planned event is not to exceed two (2) events per month.

Customer Responsibilities

- Coordinate any delivered on-site visits by Cisco, and provide minimum thirty-days (30-days) notice to Cisco of the scheduled visit; in the event the date for the scheduled visit is changed, Customer may be subject to additional charges.
- Report Severity 1 and 2 problems directly using the Cisco-provided phone number; response times do not include problems reported using Cisco.com or other electronic means.

2.5.1b. CNS High-Touch Technical Support (U.S. Only)

CNS High-Touch Technical Support (CNS HTTS) provides access to a team of network specialists who can assess and expedite issue resolution, define a Solution that seeks to limit network disruption, and assist network operating staff in implementing the appropriate Solution for increased availability of Customer's mission-critical business infrastructure.

CNS HTTS will deliver all Services by United States (US) citizens, in secure US locations, with strict data access controls in place. All Customer data is stored on network with strict access controls.

Target Customer Segment

- US Government Agencies, or Small to Medium companies operating on classified networks.
- Non-Federal US Government Entities, or Small to Medium Companies with strict security requirements.

Dependencies

- In order to purchase CNS High-Touch Technical Support, CNS High-Touch Operations Management is required across Customer's entire network.
- Depending upon the clearance level required, Service may begin thirty (30) days after acceptance of the Purchase Order.
- Customers on either unclassified or classified networks, the CNS HTTS Service will be remotely delivered from the CNS secure data center, located in Research Triangle Park, North Carolina.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Unified Communications
- Video Collaboration

- Storage Area Networking
- Data Center Switching
- Network Security
- Security Policy and Access

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Software Defined WAN
  - Network Management and Orchestration
  - Routing and Switching

Additional Information to be Collected

- Organizational structure, Solutions goals, business, technical and operational requirements.
- Security policy, security incident management process and incident handling procedures.
- Asset classification and prioritization documents.
- Information and or policies regarding normal and permissible network traffic.
- Documentation for identification, classification and prioritization of critical systems and data.
- Quarterly vulnerability scan reports which include details on listening ports, version of services, point-in-time baselines of vulnerabilities associated with critical assets such as services and software applications.
- Situations or places in the network where full packet capture may not be permissible.
- Inventory information and topology requirements, host names, IP addresses, SNMP strings, passwords, and other information necessary to activate or onboard the managed components.

Cisco Responsibilities

Project Management:

- In addition to the Cisco PM responsibilities described in the Cisco Business Critical Services - General Terms, Project Manager will:
  - Define communications flow with Customer's project sponsor and key stakeholders.
  - Review status of dependencies, risks, and issues associated with successful delivery of the Service.
  - Act as focal point for change management procedures.

Kickoff Session:

- Conduct a kickoff session which within forty (45) days from receipt of Purchase Order to review the activation process and activities with the Customer and create a project plan for activation of the Service.
- Transition monitoring and incident management of managed components:

Note: Information gathering and kickoff session must be completed before commencing the transition responsibilities:

- Transition case tracking and troubleshooting responsibilities for the supported technologies as specified on the Quote.
- Execute transition plan to transition Customer's existing network for management of the managed components by Cisco which includes the following:
- Define a high-level scope and milestones.
- Define the readiness requirements to establish connectivity and access to the managed components by Cisco.
- Define the required inventory information and topology requirements necessary to activate or onboard the managed components.
- Establish go-live date which when Cisco will begin to manage and monitor the managed components and Customer will access the Service.
- Conduct a transition out-brief upon completion of the above transition activities which will cover the following:
  - Review of incident escalation process.
  - If applicable recommendations which must be addressed based on information analyzed.
  - Service go-live date for monitoring and incident management by CNS HTTS.

Monitoring and incident management of managed components:

- CNS HTTS is provided remotely (not onsite) and includes providing the Customer direct access to the Federal Special Secure Support Team via a Cisco provided phone number. CNS HTTS will provide response to Customer as follows:
    - Severity 1 or Severity 2 calls: Response objective within fifteen (15) minutes.
    - Severity 3 or Severity 4 calls: Response objective within sixty (60) minutes.

Note: Response times do not include problems reported using Cisco.com or other electronic means.

- Provide case tracking and troubleshooting Services, where available, on a twenty-four (24) hours per day, seven (7) days per week.
- Provide 24/7 access to expert engineers, familiar with Customer's network for faster issue resolution.
- Provide network service level support which assesses services requests beyond device level to determine and address symptoms at a network level.
- Provide a dedicated toll-free number. Customer will only be asked for Service Contract number and basic information on Customer CCO profile.
- Monitor the managed components identified in transition plan.
- Provide incident handling as follows:
    - Create incident tickets on the Customer Portal.
    - Classify each ticket based on a modified version of the US-CERT incident categories located here:
    - https://www.us-cert.gov/government-users/reporting-requirements
    - Prioritize all incidents, based on information known to Cisco at the time of the incident creation into High, Medium, and Low priority and several criteria such as type of infection, confirmation of the incident, or the number of assets associated with the incident. Priorities are defined as:
    - High - Critical business impact or data loss to the Customer.
    - Medium - Adverse effect to the Customer, potential data loss, potential loss of service.
    - Low - Minimal adverse impact to Customer. No financial loss. No data loss.
    - Electronically notify designated Customer contacts for new incidents.
    - Provide mitigation recommendations as available for associated incident.
    - If Cisco becomes aware of an incident, Cisco will attempt to notify the Customer designated point of contact for the Service.

Deliverables

- Transition Plan
- Transition Out-Brief

Customer Responsibilities

- Collaborate with Cisco NCE to create the following if they do not exist for purposes of assisting with issue resolution and implementation of appropriate Solutions:
    - Topology map with IP networks
    - Design and configuration templates
- Perform tasks identified in the Transition plan in support of activation of the Service.
- Provide reasonable electronic access to Customer's network for Cisco to provide the Service.
- Report Severity 1 and Severity 2 problems for managed components using the Cisco provided phone number.
- Review incident tickets on the Customer Portal and provide timely information required for ticket resolution and closure
- Implement Cisco's recommended mitigation Solutions in a timely manner in order to expedite resolution of incidents and increase availability of Customer's mission-critical business infrastructure.

Definition of Terms Used

- **Customer Portal** – Web application provided by Cisco to Customer that details visibility into the CNS HTTS Service, including incident tickets and reports.
- **Incident Tickets** – An enumerated report that provides details about an incident detected by the CNS HTTS team and requires attention from the Customer.

- **ISO** – International Standards Organization
- **Security Incident** or **Incident** – A single series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security (ISO 27035).

3. THREAT MITIGATION

Threat Mitigation assists with aspects of incident readiness and response.

SECTION NAVIGATION

Threat Mitigation includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

3.1. Security Incident Response

Security Incident Response focuses on incident readiness and response to incidents through targeted activities that evaluate awareness and response process.

3.1.1. Security Incident Response Retainer

Security Incident Response (IR) Retainer provides review and evaluation of Customer's incident readiness program.

Architecture Supported

- Security

Additional Information to be Collected

- Incident response strategy information, including processes and workflows.

Cisco Responsibilities

- Provide one or more of the following Security Incident Response Deliverables as part of the Retainer:
- Incident Readiness Assessment, Incident Response Strategy and Planning (e.g. incident response plans, playbook), Tabletop Exercises, Proactive Threat Hunting, Compromise Assessment
- Emergency Incident Response which can include triage, coordination, investigation (such as analysis and forensics), containment, and remediation.
- Provide emergency access to Incident Response Services for the duration of the subscription.
- Use commercially reasonable efforts to (a) assign a resource within four (4) hours remotely via telephone, and (b) begin deployment of personnel to Customer location within twenty-four (24) hours.
- Provide monthly status update specific to the Customer's incident response status.

Deliverables

The Deliverables for the Service may include one or more of the following:

- Incident Readiness Assessment Report
- Incident Response Strategy and Plan Document & Playbook
- Tabletop Exercises Report
- Proactive Threat Hunting Report
- Compromise Assessment Report
- Emergency Incident Response Report

Limitations

Note: Cisco Business Critical Services General Terms - Cisco General Responsibilities - Limitations specific to Security Incident Response Retainer Service.

3.1.2. Security Incident Response Retainer Enhanced

Security Incident Response (IR) Retainer Enhanced focuses on incident readiness and response to incidents through targeted activities that evaluate prevention, detection, and response capabilities.

Architecture Supported

- Security

Additional Information to be Collected

- Incident response strategy information, including processes and workflows.

Cisco Responsibilities

- Provide one or more of the following Security Incident Response Deliverables as part of the Retainer Enhanced:
  - Incident Readiness Assessment, Incident Response Strategy and Planning (e.g. incident response plans, playbook), Tabletop Exercises, Proactive Threat Hunting, Compromise Assessment,
  - Emergency Incident Response which can include triage, coordination, investigation (such as analysis and forensics), containment, and remediation,
  - Evaluate the Customer's attack prevention and detection capabilities through a Purple Team Assessment of a device and network segment.
- Provide emergency access to Incident Response Services for the duration of the subscription.
- Use commercially reasonable efforts to (a) assign a resource within four (4) hours remotely via telephone, and (b) begin deployment of personnel to Customer location within twenty-four (24) hours.
- Provide monthly status update specific to the Customer's incident response status.

Deliverables

The Deliverables for the Service may include one or more of the following:

- Incident Readiness Assessment Report
- Incident Response Strategy and Plan Document & Playbook
- Tabletop Exercises Report
- Proactive Threat Hunting Report
- Compromise Assessment Report
- Purple Team Assessment Report
- Emergency Incident Response Report

Limitations

Note: Cisco Business Critical Services General Terms - Cisco General Responsibilities - Limitations specific to Security Incident Response Retainer Enhanced Service.

4. RESIDENT OPERATIONS EXPERT

Resident Operations Expert provides Customers with Onsite Operations Support for incident management and problem management, and Operations Onsite Consulting for operations initiatives in support of reliability, security, performance and operations of Cisco application and infrastructure.

SECTION NAVIGATION

Resident Operations Expert includes the following Service capabilities and Deliverables, each bookmarked for easier navigation:

4.1. Trusted Advisor

Trusted Advisor provides leadership help to enable Customers to obtain the benefits of Cisco Business Critical Services for Operations capabilities with a focus on planning, coordinating, and delivering required capabilities through On Site and Remote delivery approaches.

4.1.1. Operations Onsite Consulting

Operations Onsite Consulting is provided at Customer's designated location up to five (5) days per week (pending local work restrictions) during Standard Business Hours.

Technologies Supported

- Routing and Switching
- Wireless Networking
- Network Management and Orchestration
- Computing Systems
- Storage Area Networking
- Data Center Switching
- Application Centric Infrastructure
- Data Center Orchestration and Automation
- Tetration
- Unified Communications
- Video Collaboration
- Hosted Collaboration Solution
- Customer Care
- Cloud Meetings and Messaging
- Network Security
- Security Policy and Access
- Cloud Security
- Advanced Threat
- Packet Core
- Mobility Policy and Access
- SP Video Infrastructure
- IoT Edge and Fog Compute
- Industrial Networking and Collaboration

Solutions Supported

- Network Service Orchestration
  - Network Management and Orchestration
  - Data Center Orchestration and Automation
- Self-Optimizing Network (SON)
  - Mobility Policy and Access
- Network Function Virtualized Infrastructure (NFVI)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Packet Core
- Managed Services Accelerator (MSX)
- Software Defined WAN
  - Routing and Switching
  - Network Management and Orchestration
- Virtual Packet Core
  - Packet Core
- Secure Agile Exchange (SAE)
  - Routing and Switching
  - Computing Systems
  - Data Center Switching
  - Data Center Orchestration and Automation
  - Cloud Security

- Routing and Switching
- Network Management and Orchestration
- Computing Systems

Cisco Responsibilities

- Develop an understanding of Customer's technology initiatives, requirements and provide advice and guidance in support of Customer's objectives.
- Align Customer's objectives with the Services and Deliverables ordered by the Customer.
- Gather information and requirements through meetings with the Customer in support of planning, sequencing and executing Deliverables.

Note:

- Cisco may deem it necessary to provide specific Deliverables through a combination of On Site consulting and Remote-support.
- Customer-directed tasks to be performed by the Cisco Network Consulting Engineer shall be governed by the Service and Deliverables ordered by the Customer and are subject to Cisco approval, which shall not be unreasonably withheld.

Deliverables

Deliverables supported by Onsite Consulting are based on the Cisco Business Critical Services for Operations Deliverables specified in the Quote for Services ordered by the Customer, which may include the following:

Platform Insights	• Configuration Best Practices • Hardware Lifecycle Milestones • Diagnostic Analysis • Field Notices • Audit
Software Lifecycle Management	• Software Management Process and Procedure Development • Software Analysis and Release Standards • Software Track Conformance • Software Lifecycle Milestones • Product Security Advisory Customer Impact Assessment
Technology Assessments	• Resiliency Assessment • Collaboration Security Assessment • RF Verification Assessment • WLAN RF Assessment
Operations Management	• Escalation Engineering Support
Knowledge Management	• Knowledge Transfer Session for Operations
Instrumentation Management	• Management Instrumentation Review • Management Deployment Planning and Readiness Assessment

Customer Responsibilities

- Provide Cisco with direction of activities, projects, and priorities on which the Customer needs the Cisco Engineer to engage.

4.1.2. Operations Onsite Support

Operations Onsite Support is provided at Customer's designated location up to five (5) days per week (pending local work restrictions).

Operations Onsite Support is only available in certain geographic locations and will be specified in the Quote for Services.

Solutions Supported

- Expert Care

Cisco Responsibilities

- The responsibilities provided by Operations Onsite Support are defined within the following Deliverables described above.

Operations Management	• Incident Management • Problem Management- High-Touch Engineering

Note: Cisco may deem it necessary to provide specific Deliverables through a combination of On Site Support and Remote-support.

Deliverables

- Onsite Support Incident Management
- Onsite Support Problem Management High Touch Engineering

Note: The Quote will specify the Operations Onsite Support Deliverables(s) purchased.

Customer Responsibilities

- Provide Cisco with direction of support activities and priorities on which the Customer needs Cisco Support to engage.