REMEDIATION RETAINER SERVICE

Last Modification Date: 03/13/2024
Exported and Shared on: 03/13/2024

For additional information, visit www.intervision.com

CONTENTS

REMEDIATION RETAINER SERVICE

Description

Remediation Retainer Service is designed as a nonemergency service to take action based on recommendations from security services such as Penetration Testing as a Service(PTaaS), Detection and Response Services (MDR,XDR), Managed Endpoint Protection Services, and Managed Vulnerability and Risk Services.

In Scope

- Remediation and restoration to normal operating conditions, testing and documenting each fault within the InterVision trouble ticket system via change enablement. (MACD)
- Ownership of resolution of the problem on behalf of the Customer and act as an agent for the Customer under executed letters of agency
- Notify the Customer of the progress of all milestones per the client-provided contact process.
- Assistance with vendor escalations.
- Safeguard customer's proprietary information using commercially reasonable efforts to securely access the client network through an encrypted tunnel.
- ***If, during the life cycle of the contract, a device becomes “Out of Scope / Unsupported”, Operational Support will be reduced to the following:
    a. Device replacement (client-provided device or new purchase) with existing configuration included.
    b. Additional remediation at T&M.

1. Actions related to Device Failures, including those due to failed recovery during the InterVision execution of Client Approved changes, are limited to:
2. The risks of operating Unsupported Software with known vulnerabilities that cannot be addressed due to the lack of vendor support are considered “Accepted” by the client.
3. All Operations Center related Incident Remediation efforts are limited to two hours in scope within standard contract language; any additional efforts are subject to T&M.
4. Hardware Component failures are the responsibility of the client or must be addressed through T&M / Dispatch.

Out of Scope

- Software licenses and subscriptions are not included. Management devices and software provided as part of the Managed Service will be licensed.
- Configuration changes to covered devices that are not recommendations from detection and response services (MDR, XDR, EDR). Or Vulnerability Management Platforms (Arctic Wolf Managed Risk, and Penetration Testing as a Service powered by RedSpy365)
- Coverage for devices not under the agreement are ineligible for support of any type.
- Remediation activities to ensure detection and response infrastructure is available.

Customer Requirements

To allow for successful monitoring and management of devices and execution of SLAs, Customer responsibilities include:

- Providing all network and device information for the InterVision Managed Services team and tools to discover the contracted devices. This information includes network diagrams, site information, circuit information, and Customer Vendors, Letters of Agency, and current software levels.
- Providing computing resources to run InterVision's access and management tools, and the means for the Collector to contact the InterVision Data Center.
- Performing configuration of devices and network, as necessary, to facilitate management of the contracted devices. In the event, that the customer is unable or does not have the personnel to enable management of devices, InterVision's Professional Services can be engaged for assistance at an incremental cost.
- Provide device access - Remote access to devices must be available for support. The client is responsible for out-of-band access, along with in-band access.
- Provide a distribution list of Customer contacts

- Supply InterVision team with all the necessary security information including dial-in numbers, access IDs, and passwords, necessary for InterVision to perform the Services
- Provide notification contact and escalation lists for use by InterVision during business and non-business hours.
- Provide InterVision team with site contact to facilitate access to equipment and connection terminations, along with out-of-hours access procedures
- Notify InterVision within 72 hours of any changes to the contracted devices via a service/change ticket.
- Execute letters of agency notifying vendors, such as carriers, that InterVision will represent the Customer
- All devices and applications must have vendor support contracts and operate at currently supported vendor versions.
- All devices must be in a supportable state, including current versions of software supported by the vendor, with all critical patches applied, in a production-capable state with no known failures or functions in order to be covered. Remediation efforts to bring software to the current version including patches to make a device production capable will be billable to the customer.

1 ROLES AND RESPONSIBILITIES MATRIX

"X" indicates the responsible party. "*" indicated optional services.

Remediation Roles and Responsibility Matrix	Customer	InterVision Remediation Service	Extended Service (Separate Managed Service)*
General			
Device information (account. password, location, MAC address,…)	X		
Client escalation information	X		
Vendor support contracts	X		
**Audit the Network environment for configuration issues, vulnerabilities, and risks.			X
Installation and Configuration			
The initial design, installation, and configuration of the Device	X		
Monitoring			
Setup, configure, and continual monitoring of all devices			X

REMEDIATION RETAINER SERVICE

Case Management			
Change management for remediation		X	
Reason For Outage (circuit only)			X
Root Cause Analysis			X
Vendor management (Escalations, RMA,...)		X	X
Troubleshoot performance and availability			X
Patch Management			
Firmware and patching updates for remediation		X	
Regularly scheduled patching	X		X
Management			
Administer device accounts	X		
Administer user access	X		
Performance tuning and management (bi-annual)	X		X
Capacity / Bandwidth analysis (bi-annual)	X		X
Life Cycle Management Notification (bi-annual)	X		X
Backup and Rollback	X		X
Reporting (Reporting will be provided through Detection and Response services)			
Standard Reports			X
Custom Operations Reports			X

* Optional services capability that can be provided with incremental fees. These services may be additional managed or professional services.

** This item requires a paid on-boarding fee specifying assessment or audit in the description.

Service Levels

- Service offers 24/7/365 ticket support.

Service Activation

InterVision employs a structured process to help ensure a smooth transition to Managed Remediation Services. Our Project Management Office (PMO) owns the process with the Onboarding Engineer (OE), holding the ultimate responsibility and serving as the single point of contact (SPOC).

Steps to activate service

1. Data gathering

1. Customer service manual
2. Order form

- Access collector/ Support workstation Deployment and Configuration
- Onboard customer devices
- Add data from step one into systems
- Finalize customer onboarding
- Send any found issues with onboarding for client to review

2 GO LIVESERVICE ACTIVATION

InterVision employs a structured process to help ensure a smooth transition to Managed Infrastructure and Monitoring services. Our Project Management Office (PMO) owns the process with the Onboarding Engineer (OE), holding the ultimate responsibility and serving as the single point of contact (SPOC).

Steps to activate service

1. Data gathering

1. Customer service manual
2. Order form

- Monitoring collector/ Support workstation Deployment and Configuration
- Onboard customer devices
- Add data from step one into systems
- Finalize customer onboarding
- Send any found issues with onboarding for client to review
- Go Live/ Customer training
- Perform true-up / Project Closeout

Network Infrastructure Evaluation

For new client environment onboarding not recently set up by InterVision Services, an evaluation is required that will review the environment to ensure it is in a supportable state. Software and Firmware will be reviewed to be current or within one major software version behind current. This evaluation will also review configuration, and access control policies for critical risks. Software/Firmware, configuration, and access control issues and risks must be addressed to be in a supportable state. Environment updates may be identified as requiring additional project time via a separate scope of work to address and InterVision reserves the right to modify SLAs or refuse service if Environments are not current and critical risks addressed.

Service Level Agreements and contract language can all be found in the Managed Services Statement of Work (MS-SOW)

Service Level Objectives (SLO) for Resolution Retainer Services

SLA Metric	MACD Urgent	MACD Standard	MACD Scheduled
Resolved within:	48 Hours	72 Hours	Scheduled

Severity Table Map

Priority Level	Urgent*	Standard*	Scheduled
Arctic Wolf	Critical	High	Medium and Low
CyberSafe	Critical	High	Medium and Low
InterVision	Critical	High	Medium and Low
RedSpy365	Critical	High	Medium and Low

*If Critical or High-level incidents require scheduling an outage then they should be considered Scheduled with minnimum 72hrs notice.

Service Items

Security Remediation Services 5 Hours a Month	Bucket of hours that can be utilized monthly to help with remediation activities on devices.
Security Remediation Services 10 Hours a Month	
Security Remediation Services 15 Hours a Month	
Security Remediation Services 20 Hours a Month	
Remediation Service Network Device	Remediation License for a network device
Remediation Service Server and Host Device	Remediation License for a Server or Host device

Remediation Service Workstations Device	Remediation License for a Workstation device
Security Remediation Services overages	Hourly billing for consumption of services beyond the size of the monthly retainer

3 REMEDIATION RETAINER SERVICES SUPPORTED DEVICES:

Managed Services Supported Products and Devices

Managed Network Services[1]

Supported Products:

Arista Switches

Cisco Aironet

Cisco Meraki Cameras (requires support of the Meraki network environment)

Cisco Meraki MR Wireless LAN**

Cisco Meraki MS Switching**

Cisco Meraki MX Router**

Cisco Routers* – ASR / ISR / Catalyst 8k

Cisco Switches – Catalyst

Cisco Switches – MDS Multilayer 9000 Series

Cisco Switches – Nexus 3000, 7000, 9000 Series (ACI functionality and controllers supported as Essential only)

Cisco Switches – Small Business 300 Series

Cisco UCS Fabric Interconnects 6200 Series

Cisco VG300 Series Gateways

Cisco Virtual Wireless Controller

Cisco Wireless LAN Access Points

Fortinet FortiAP

Fortinet FortiExtender (Essential only, requires next hop LAN device support)

Fortinet FortiSwitch

Fortinet FortiWifi

HP ProCurve Switches

HP Aruba EdgeConnect (Silver Peak) SD-WAN - Router

HP Aruba Switches

HP Aruba Wireless Access Points

HP Aruba Wireless Management

Juniper Switches - EX Series

Juniper Switches - MX Series

Cisco Email Security Appliance (MONITOR ONLY Service)

End of Support & End of Life:

Riverbed Xirrus

1 https://intranet.intervision.com/display/PT/Managed+Collaboration+Services

*Cisco Router support does not currently include SD-WAN updates and management (under development)

** Cisco Meraki environments requiring two-factor authentication to log into the management dashboard are not supported

Managed Security Services[2]

Supported Security Appliances:

CheckPoint Firewall

Cisco Adaptive Security Appliance (ASA) Firewall

Cisco FirePower Management Center (FMC)

Cisco FirePower Threat Defense (FTD) Firewalls

Cisco Meraki MX firewalls*

Fortinet FortiGate Firewall

Fortinet FortiManager

Palo Alto Next Generation Firewall

Palo Alto Panorama Management Console

Available through custom SOW:

Aruba ClearPass

Cisco Duo

Cisco Umbrella DNS

* Cisco Meraki environments requiring two-factor authentication to log into the management dashboard are not supported

Managed Server and Storage[3]

Supported Products:

Cisco UCS Fabric Interconnects 6200 Series

Cisco UCS B Series Hardware

Cisco UCS C Series Hardware

Dell/EMC VNX Storage (Not VNXe)

Microsoft Active Directory

Microsoft Windows Server 2016

Microsoft Windows Server 2019

Microsoft Windows Server 2022

NetApp Filer Storage - FAS

VMware VMware ESX

VMware vCenter

Support Only, No Monitoring:

Microsoft O365 (O365 must be purchased from Hosted Cafe to gain support)

Monitor Only

APC-Schneider Electric UPS

CentOS 6 & 7

Debian Linux 8 & 9

Redhat Enterprise Linux 6, 7, 8

Ubuntu Linux 14.04 LTS, 16.04 LTS, 18.04 LTS

End of Support / End of Life:

2 https://intranet.intervision.com/display/PT/Managed+Firewall+Services
3 https://intranet.intervision.com/display/PT/Managed+Server+and+Storage

	Nimble Storage
	Pure Storage

*Unsupported devices will require extended services and the objectives and deliverables of this service guide do not apply.