STATEMENT OF SERVICE

Name: Kurt Simpson

Phone: +1 206-823-5285

Quote Date: 04-02-2025

Quote Expiration: 05-02-2025

Quote ID: Q-18309-1

Bill To:

Name: Aaron Fry

Company: City of Fullerton

Address: 303 W. Commonwealth Ave
Fullerton, CA 92832

Phone: (714) 738-6300

Ship To:

Name: Aaron Fry

Company: City of Fullerton

Address: 303 W. Commonwealth Ave
Fullerton, CA 92832

Phone: (714) 738-6300

SERVICE SUBSCRIPTION (RECURRING SERVICES)

SKU	Description	MSRP	Discount	Duration	Qty	Annual Net Price
CI-MDR-FULL-5-50	MDR Comprehensive: Lumifi Cyber's 24x7 Security Operations Center ingests and monitors key events and alert data to detect and respond to malicious activity. MDR Comprehensive includes the monitoring of supported Endpoints, Office 365, On-Prem, AWS, and/or Azure. If threats are identified, CI will quarantine endpoints and users based on criteria in pre-approved playbooks. Collectors must be subscribed to separately (Users Up to 50).	$26,400	44%	36	50	$14,784
CI-MDR-FULL-5-51-1000	MDR Comprehensive: Users 51-1000	$92,400	44%	36	700	$51,744
CI-MDR-FULL-10GB	Includes the monitoring and ingest of MDR Comprehensive & all additional Windows Event Logs and access to Lumifi's full suite of integrations for ingest. Ingest of 10 Gigabytes per day for additional integrations.	$6,600	44%	36	1	$3,696
CI-P: ROBO	ROBO (Remote Office/Branch Office) Collector(s): To monitor On-Prem environments, Lumifi Cyber will provide and manage collector(s) for the duration of the service.*	$4,356	44%	36	1	$2,439.36
CI-P: 1U	1U Collector(s): To monitor On-Prem environments, Lumifi Cyber will provide and manage collector(s) for the duration of the service.*	$12,200	49%	36	2	$6,222.00
CI-P: 4U	4U Collector(s): To monitor On-Prem environments, Lumifi Cyber will provide and manage collector(s) for the duration of the service.*	$46,200	44%	36	1	$25,872
One-time Setup	MDR Platform Setup Fee* [1]			1	1	$0

*Line items subject to Sales Tax and are not included in this quote.

[1]Item invoiced when the project reaches the associated Milestone. Refer to Scope of Work for Milestone descriptions.

[3]Internal Reference

	Summary
Year 1 Total:	$104,757.36
Year 2 Total:	$104,757.36
Year 3 Total:	$104,757.36
Total Contract Value:	$314,272.08

TERMS AND CONDITIONS

This Statement of Service ("*SOS*"), effective as of 06-02-2025 (the "*Effective Date*") is subject to the Lumifi Terms & Conditions, the Lumifi Cyber, Inc. Description of Service attached here as Exhibit A, and any other Exhibits, Attachments or Amendments hereto, which are each incorporated herein by reference, and which together with this SOS constitute the "*Agreement*". Unless otherwise provided in this SOS, capitalized terms herein shall be as defined elsewhere in the Agreement. The terms of this Agreement constitute the final expression of the parties' binding understanding in respect to the subject matter hereof and supersede all prior or contemporaneous agreements, representations and understandings, written and oral, in respect to same. **Customer acknowledges that it has read the Agreement and agrees to be bound by its terms.**

- The term of this SOS is 36 month(s) commencing the Effective Date hereof, which upon expiration shall automatically renew for successive annual renewal terms until terminated as provided in the Lumifi Terms & Conditions.
- Billing shall be based on Lumifi Cyber reporting. Lumifi Cyber and Customer shall reconcile in good faith any discrepancies in their respective tracking records, provided Lumifi Cyber's reporting shall control in the event of an irreconcilable discrepancy.
- Customer shall be invoiced on an annual basis in advance for Recurring Services and upon Milestone completion for One-time Services.
- The first invoice shall be issued following the Effective Date.
- Payment of invoiced amounts due no later than thirty (30) calendar days from date of invoice.
- Additional Data: No charge for up to 540.00 GB/month. If the total data for MDR services (CI-P & CI-MDR SKUs) in a given month exceeds this amount by more than 10%, an overage fee of $2.17 per gigabyte (GB) shall be charged for all overage amounts. Data overages shall be invoiced in arrears on a monthly basis and payment thereof shall be due and payable net 30 days from the date of invoice.

Check one of the following:

☐ Purchase Order Required
☐ Purchase Order Not Required

Customer Signature _____

Name _____

Title _____

Date _____

Billing Contact Name _____

Billing Street Address _____

City, State, Zip _____

Billing Contact Phone _____

Billing Email _____

Lumifi Cyber, Inc. Signature _____

Name _____

Title _____

Date _____

Internal Information
Affiliate: N/A

EXHIBIT A
LUMIFI CYBER, INC. ("LUMIFI") DESCRIPTION OF SERVICE

LUMIFI CYBER COMMERCIALLY AVAILABLE PRODUCTS V. DECEMBER 2024		
SERVICE ID	DESCRIPTION	AVAILABILITY
CI-MDR	MANAGED DETECTION AND RESPONSE	GENERALLY AVAILABLE
CI-P	ON-PREMISES COLLECTOR	GENERALLY AVAILABLE
CI-P-VM	VIRTUAL SENSOR (10G,1G,500M or 200M extension based on bits/second throughput)	BETA
CI-P-SENSOR	SERVER SENSOR FOR LINUX SERVERS	BETA
CI-CVI	ON-PREMISES VULNERABILITY SCANNING	GENERALLY AVAILABLE
CI-LR	LOG RETENTION FOR ON-PREMISES SYSTEMS	GENERALLY AVAILABLE

THIS DESCRIPTION OF SERVICE INCLUDES ALL LUMIFI CYBER ("LUMIFI") GENERALLY AVAILABLE COMMERCIAL OFFERINGS FROM LUMIFI. "GENERALLY AVAILABLE" PRODUCTS & SERVICES ARE SUBJECT TO THE SERVICE LEVEL COMMITMENTS OR "SLA'S" SET FORTH IN THE SERVICE LEVEL AGREEMENT SECTION. HARDWARE, PRODUCTS & SERVICES LISTED AS "ALPHA" OR "BETA" ARE *NOT* SUBJECT TO ANY SLA'S. ALPHA/BETA PRODUCTS & SERVICES ARE PROVIDED 'AS IS' WITH NO WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. LUMIFI SHALL USE COMMERCIALLY REASONABLE EFFORTS TO SUPPORT ALPHA AND BETA PRODUCTS & SERVICES ONLY ON AN 'AS AVAILABLE' BASIS.

YOU MAY NOT HAVE PURCHASED ALL PRODUCTS & SERVICES OUTLINED IN THIS DOCUMENT, PLEASE SEE YOUR STATEMENT OF SERVICE FOR A LISTING OF THE SERVICES YOU HAVE PURCHASED. THE SECURITY PRODUCTS AND LOGS THAT ARE MONITORED FOR CUSTOMER PURCHASED SERVICES ARE DOCUMENTED IN THE INTEGRATION LIST, WHICH DETERMINES THE IN-SCOPE SOURCES. CHANGES TO THE INTEGRATION LIST CAN OCCUR BASED UPON MUTUAL WRITTEN AGREEMENT (EMAIL SUFFICES) BETWEEN LUMIFI AND THE CUSTOMER. LUMIFI'S PRICING IS BASED ON THE ENVIRONMENTS THAT ARE MONITORED; ANY ADDITIONAL PRODUCTS, LOGS, OR ENVIRONMENTS THAT INTRODUCE NEW DATA MAY RESULT IN ADDITIONAL SUBSCRIPTION FEES. SOME LUMIFI PRODUCTS & SERVICES, SUCH AS MDR & LOG RETENTION, ARE SUBJECT TO MAXIMUM DATA TRANSFERS OVER CERTAIN TIME PERIODS. THESE LIMITS ARE DOCUMENTED ON YOUR STATEMENT OF SERVICE. OVERAGE CHARGES WILL APPLY TO DATA TRANSFERS EXCEEDING CONTRACTED MAXIMUM. SEE BELOW FOR MORE INFORMATION.

SERVICE DESCRIPTION

Lumifi Cyber's Cybersecurity-as-a-Service provides a comprehensive set of cybersecurity services for organizations. This document outlines LUMIFI's **Managed Detection & Response (MDR)**, where LUMIFI monitors customer environments for threats and provides notification & response if threats are detected. Additional add-on services are also described in this document, such as **Log Retention (LR)** and **Continuous Vulnerability Identification (CVI)**. A full listing of Customer's in-scope services is listed on the Statement of Service. Professional Services work will be detailed in a separate Scope of Work.

Lumifi Cyber's MDR service is built to both monitor customer's existing security products, along with complimenting those products with additional services such as LUMIFI-supplied Collector(s), Virtual Sensor(s) and a 24x7 SOC. The in-scope **Log Sources, Products, and Services** that LUMIFI will monitor as part of the MDR service for the Customer are documented in the **Integration List.** The level of services that LUMIFI can provide depends both on the product capabilities that the customer is licensed for (i.e. Microsoft license level, licensed 3rd-party Endpoint Detection and Response (EDR) capabilities) and what LUMIFI's service is set up to support.

Lumifi Cyber's **Collector** installed on LUMIFI owned and managed hardware allows LUMIFI to monitor network traffic for on-premises environments. The Collector includes an intrusion detection system to monitor for threats, allows Customer to transfer syslogs and Windows events to LUMIFI, along with providing continuous packet capture for LUMIFI to review throughout the MDR service.

Lumifi Cyber's **Virtual Sensor** for deployment on Customer-owned and -managed hypervisors allows LUMIFI to monitor network traffic for on-premises networks without deploying new LUMIFI hardware. The Virtual Sensor, which comes as a virtual machine image includes an intrusion detection system, deep packet inspection and a threat sandbox to monitor for threats and allows Customer to transfer syslogs and Windows events to LUMIFI.

Lumifi Cyber's **Linux Server Sensor** for deployment on Customer-owned and -managed Linux Servers allows LUMIFI to monitor Linux Servers without deploying new LUMIFI hardware (NOTE: the Linux Server Sensor does not ship Linux logs). The Linux Server Sensor, an agent installed by the Customer, allows LUMIFI to monitor process information, command execution, files, and file events. The Linux Server Sensor converts that information to metadata that then correlates traffic, processes, users, and commands for security, DDoS, and breach attempt detections.

Lumifi Cyber's **Log Retention** is an additional service designed and meant for long-term, secure, and compliant log storage where LUMIFI retains, encrypts, and hashes customer logs sent to LUMIFI's on-premises Collector(s). Customers can then request a time-bounded extract of their logs by submitting a request to LUMIFI.

LUMIFI's **Continuous Vulnerability Identification** service is an additional service that runs on the Collector which utilizes an industry-standard network active scanning product to identify system vulnerabilities. LUMIFI provides reports and dashboards for customers to manage their prioritized vulnerabilities.

The customer journey starts with onboarding where LUMIFI and Customer work together to integrate products to activate MDR & additional services. Lumifi Cyber will monitor the in-scope products and respond to threats as they are detected, following the Rapid Quarantine Playbooks agreed with Customer where relevant, and, where applicable, providing response playbooks to Customer based on industry best practices.

CHANGE IN SERVICE	If Customer wishes to change the scope of their service, including: • Adding additional LUMIFI Services • Changing the in-scope products or logs that LUMIFI monitors • Changing the environment LUMIFI monitors, such as adding a Microsoft tenant, AWS tenant, or adding a new Collector or Virtual Sensor Then the Customer must reach out to their LUMIFI Customer Success Manager. LUMIFI's Customer Success Manager will walk Customer through the change in service process and communicate those changes to the wider LUMIFI team to ensure accurate service delivery. A change in service may warrant an addendum to the solution design, a change to the Integration List, or may involve a change request to the existing contract, depending on the requested change. If Customer has a question about their service or has a product or service support inquiry, LUMIFI's Customer Success Manager is the correct LUMIFI contact to whom the question, inquiry or request should be directed.
DATA LIMITS	Some LUMIFI services have limits on the amount of data that can be sent to LUMIFI over a timeframe that is specified on the Statement of Service order form. If required, Customer can purchase Additional Data as they grow their business or integrate additional security products. For LUMIFI's MDR service (CI-MDR), both Customer and LUMIFI will have Portal access to view Customer's data usage. The Customer will work with LUMIFI in good faith to reduce data usage once contracted monthly data limit has been achieved. Data usage overages will be billed in accordance with the Statement of Service. For LUMIFI's Log Retention service (CI-LR), LUMIFI will work with Customer to ensure that their current usage is known to ensure that Customer's annual logs retained align with expectations. If Customer is forecasted to go over their annual allotment, LUMIFI will work with Customer to better refine the logs stored or additional data storage must be purchased.

CUSTOMER ONBOARDING & SERVICE ACTIVATION	
MDR ONBOARDING & ACTIVATION (CI-MDR)	Lumifi Cyber's onboarding process starts from the effective date of the Statement of Service and lasts until the last security product is activated. Lumifi Cyber will work with Customer throughout the process, provide documentation and assistance, and provide reasonable assistance for 3rd party product integration. The list of Customer's in-scope products that will be onboarded for the Managed Detection & Response service are documented in the Integration List. LUMIFI's onboarding obligation shall be conditioned at all times on Customer's timely engagement and support as specified herein and as otherwise reasonably required by LUMIFI. During onboarding, LUMIFI will work with Customer to establish communication protocols for response, support, incident escalation, and service reviews. Additionally, LUMIFI will finalize customer network, business, and contact information for use during the service. <u>Customer responsibilities during MDR onboarding:</u> • Provide timely responses and make reasonable resources available to ensure expedient service activation • Ensure Customer security integrations are correctly configured, and all products are set up and sending data as laid out in LUMIFI's onboarding documentation • Ensure Customer's security products are correctly configured and monitoring desired devices, accounts, and networks within Customer's environment • Ensure security products are correctly licensed for LUMIFI integration and LUMIFI actions where relevant <u>MDR is activated once the following are completed:</u> LUMIFI will verify security products by ensuring successful transfer of log and/or alert data.
RAPID QUARANTINE PLAYBOOK ACTIVATION (CI-MDR)	LUMIFI's actions are governed by the **Rapid Quarantine Playbook,** which detail when LUMIFI is authorized to take certain specified actions, when LUMIFI should not take action, and defines contact protocols. Customer can opt-in to these service components by completing the playbook. <u>Rapid Quarantine is activated once the following are completed:</u> • Customer has completed and signed, and LUMIFI has accepted, the Rapid Quarantine Playbook(s) • LUMIFI and Customer have successfully tested the agreed rapid quarantine action(s) Completing these playbooks will authorize LUMIFI to take the actions detailed in the playbook during a confirmed incident as laid out in the Rapid Quarantine Playbook. LUMIFI will provide assistance in filling out the playbooks and what the impacts of various options are. Specific recommendations or evaluation of customer environments and risk tolerances would require additional professional services, governed and charged in a separate Scope of Work.

COLLECTOR ONBOARDING & ACTIVATION (CI-P)	LUMIFI monitors on-premises environments using the Lumifi Cyber Collector (“Collector”). This physical will monitor network traffic that is provided to the device. In addition, in-scope security products can send logs to the Collector in accordance with LUMIFI’s onboarding documentation and guidance. LUMIFI will provide reasonable assistance in activating the Collector(s) and work with Customer to ensure network and Collector stability. Each Collector is sized to hold a maximum amount of data, and while additional log storage can be accommodated, there will be an additional charge if hardware or size upgrades are required during the lifetime of the service. Customer responsibilities during Collector onboarding: • Install the Collector within desired customer networks • Ensure requested firewall rules have been added or modified according to LUMIFI’s documentation • Forward in-scope logs noted on the Integration List to the Collector according to LUMIFI’s documentation • Set up Port Mirroring/Port Spanning configured to provide a full copy of network traffic included in the Solution Design or as otherwise mutually agreed between LUMIFI and Customer The On-Premises Collector service is activated once the following are completed: The On-Premises Collector is activated once LUMIFI verifies expected data is successfully being received into LUMIFI’s platforms and the Collector is operating normally.

VIRTUAL SENSOR ONBOARDING & ACTIVATION (CI-P-VM)	LUMIFI monitors on-premises environments using the Lumifi Cyber Virtual Sensor ("Virtual Sensor"). This virtual machine installed on a Customer-managed hypervisor will monitor network traffic that is provided to the device. LUMIFI will provide reasonable assistance in activating the Sensor(s) and will work with Customer to ensure network and Virtual Sensor stability. Each Sensor is sized based on the maximum network bandwidth in gigabits/second, and there will be an additional license charge if network maximum bandwidth usage exceeds Virtual Sensor's licensed requirements. <u>Customer responsibilities during Virtual Sensor onboarding:</u> • Understand how to and take responsibility for ensuring the hypervisor is properly configured to provide a Virtual IP address that can receive full span port traffic or network tap traffic ○ NOTE: LUMIFI does not provide support for installing and properly configuring a hypervisor and the network configuration of the hypervisor required to provide MDR services, and is entirely the responsibility of the Customer • Install the Virtual Sensor within desired customer networks on a virtual machine host that meets LUMIFI specifications • Ensure requested firewall rules have been added or modified according to LUMIFI's documentation • Forward in-scope logs noted on the Integration List to the Virtual Sensor according to LUMIFI's documentation • Set up Port Mirroring/Port Spanning configured to provide a full copy of network traffic included in the Solution Design or as otherwise mutually agreed between LUMIFI and Customer <u>The Virtual Sensor service is activated once the following are completed:</u> The Virtual Sensor is activated once LUMIFI verifies expected data is successfully being received into LUMIFI's platforms and is operating normally.

LINUX SERVER SENSOR ONBOARDING & ACTIVATION (CI-P-SENSOR)	LUMIFI monitors on-premises Linux Servers using the Lumifi Cyber Linux Server Sensor ("Linux Server Sensor"). The Linux Server Sensor allows LUMIFI to monitor process information, command execution, files, file events. The Linux Server Sensor converts that information to metadata to then correlate traffic, processes, users, and commands for security, DDoS, and breach attempt detections. LUMIFI will provide reasonable assistance in activating the Linux Server Sensor(s) and will work with Customer to ensure Linux Server Sensor stability. Customer responsibilities during Linux Server Sensor onboarding: • Understand how to and take responsibility for ensuring the Linux Server Sensor agent is properly configured to send data to either an on-premises aggregator or directly to Stellar Cyber ○ NOTE: LUMIFI does not provide support for installing and properly configuring a Linux Server, and is entirely the responsibility of the Customer • Install the Linux Server Sensor the desired customer Linux Server • Ensure requested firewall rules have been added or modified according to LUMIFI's documentation The Linux Server Sensor service is activated once the following are completed: The Linux Server Sensor is activated once LUMIFI verifies expected data is successfully being received into LUMIFI's platforms and is operating normally.
CVI ONBOARDING & ACTIVATION (CI-CVI)	If Customer has purchased the add-on Continuous Vulnerability Identification service in addition to a Collector, LUMIFI will configure the Collector for this service prior to shipping the Collector. Customer responsibilities during CVI onboarding: • Provide list of targets for the CVI scans, i.e. IP Ranges, subnets etc. • Enable any internal firewall rules needed for vulnerability scanning behind firewalled internal networks • Provide Domain Admin credentials if credentialed scanning is desired (multiple secure methods are available) CVI is activated once the following are completed: The scanner license is activated on the Collector and has LUMIFI has confirmed the configuration and enabled scans are being received as expected.

LOG RETENTION ONBOARDING & ACTIVATION (CI-LR)	If Customer has purchased the add-on Log Retention service, there will be some additional setup by both the Customer & LUMIFI to ensure Customer logs are being retained. LUMIFI will configure the Collector for this service prior to shipping the product.
	
	<u>Customer responsibilities during Log Retention onboarding:</u>
	• Customer will configure their log sources to send to LUMIFI's Collector
	• Customer will complete LUMIFI deployment documentation:
	  ○ In-scope log sources
	  ○ Static IP(s) of the host(s) forwarding logs to LUMIFI's Collector
	  ○ Time zone of the log source for accurate pulling of logs during the service
	
	<u>Log Retention is activated once the following are completed:</u>
	LUMIFI verifies reception of all in-scope customer logs to LUMIFI's data store.

LUMIFI SERVICES & COMPONENTS	
MDR OVERVIEW (CI-MDR)	Once activated, Lumifi Cyber's MDR service provides 24x7 detection & response. The MDR service contains the following service components, with the actual service components activated depending on Customer's in-scope products and services: • Case Review • Event Monitoring • Threat Hunting • Response • Rapid Quarantine • Service Reviews • XDR Alerts • Dashboard & Portals • Support Request LUMIFI tailors its MDR services to Customer's activated security products. The exact components, data, alerts, and logs available for LUMIFI services will vary depending on the activated security products. LUMIFI's SOC will not utilize Customer's security product's dashboards or portals, but instead will utilize the integrations to receive data and execute actions. A list of Customer's in-scope security products can be found in the Integration List. The procedures for changing Customer's service are included in the Change of Service section at the top of this document. <u>Customer Responsibility during the lifetime of the MDR service:</u> • Timely response to LUMIFI communications • Ensuring Customer security products are correctly configured & monitor the in-scope networks, devices, and accounts • Promptly communicating changes, if any, to the monitored customer network to LUMIFI's SOC and LUMIFI's Customer Success Manager

CASE REVIEW (CI-MDR)	LUMIFI will monitor in-scope security products and elevate select alerts for SOC review as "Cases". Alerts that LUMIFI raises to manual SOC review are based on LUMIFI's determination of cyber risk which is a combination of advanced analytics scoring along with LUMIFI and Customer service history. The ultimate goal of Case creation and review is to ensure there are multiple detection points for a given threat, while minimizing false positives for both LUMIFI and Customer. LUMIFI's SOC will investigate Cases and corresponding alerts using all in-scope security products for a Customer's MDR service, as relevant to the investigation. Multiple alerts may be grouped into a single investigation through correlation and automation or through SOC investigation. LUMIFI will assess the threat of an investigation based on mapping the outcome of a thorough investigation with the Incident Classification and SOC Severity Matrix. LUMIFI will use underlying alert severities and risk scores as guides but will ultimately determine the threat level of an investigation based on SOC expertise, analytics, and processes. All alerts that have been escalated to the SOC for review in Cases will be reviewed in alignment with the MDR SLA's outlined in the Service Level Agreement section at the end of this document. If LUMIFI confirms an incident, which involves a LUMIFI analyst verifying evidence of an attack or threat actor, Customer will be notified as agreed during deployment. If the confirmed incident has at-risk assets that are covered by Rapid Quarantine, LUMIFI will act according to the agreed playbook(s).
EVENT MONITORING (CI-MDR)	Many integrations include raw audit and security events that LUMIFI uses for additional XDR detections of threats, for contextual information during investigations, or to determine normal behavior patterns of systems. While events are crucial, they are also the primary driver of data volumes sent to LUMIFI, so it is important that only security-relevant events are sent to maximize the value of Customer's MDR service. <u>Customer responsibility for in-scope products:</u> • Correctly configure Customer's products to only send security relevant events and alerts • Stay within Customer's contracted data limits • Work with LUMIFI if Customer is forecasted to exceed, or exceeds, the contracted data limits and promptly pay for invoiced overages
THREAT HUNTING (CI-MDR)	LUMIFI will engage in threat hunting activities at its discretion. Typical reasons include: • Enhanced Monitoring for at-risk assets • Scanning customer environments during large-scale cyber incidents • Automated threat hunting results review • Periodic reviews of customer networks at Customer request LUMIFI will utilize all in-scope security products to investigate Customer's networks via LUMIFI analytics tools. Unusual findings will be escalated to Customer and/or discussed during Service Reviews.

RESPONSE (CI-MDR)	If LUMIFI confirms an incident during Case Review or Threat Hunting, LUMIFI will notify Customer within the specified Service Level Agreement section. If the in-scope assets are covered by the LUMIFI Rapid Quarantine service component, LUMIFI will take response actions in-line with the agreed playbook(s). LUMIFI will follow the contact procedures outlined during Customer onboarding for contact procedures during response, including method of contact and who to contact depending on incident severity. LUMIFI will provide context and recommended next steps for lower severity investigations. LUMIFI also has a number of playbooks that will be included for common threat behaviors. For urgent or high severity incidents, a final Incident Report will be delivered to Customer at the time that all related tickets are closed. The report will include: • Summary of incident • Summary of any confirmed actions taken (by LUMIFI and/or Customer) • Final status and/or resolution <u>Customer Responsibility during Response:</u> • Following cybersecurity best practices or LUMIFI's recommended playbook steps • If Customer thinks this is a false positive, notifying LUMIFI and providing supporting details will allow LUMIFI to deliver better services for future notifications • Informing LUMIFI if an alternative method of notification is preferred
RAPID QUARANTINE (CI-MDR)	The Rapid Quarantine service allows LUMIFI to block at-risk users through in-scope Identity Providers (i.e. Microsoft Entra ID), or isolate at-risk hosts though in-scope EDR's. If Customer has opted into the Rapid Quarantine service component and activated it by completing the steps outlined in the MDR Deployment section, LUMIFI will utilize the agreed playbook(s) during confirmed incidents. LUMIFI will take actions governed by the mutually agreed Rapid Quarantine Playbook when any investigation reaches the thresholds determined in the playbook. LUMIFI will take no action in Customer's environments that is not detailed in the agreed playbook(s). LUMIFI's actions as detailed in the Rapid Quarantine Playbook may include, but are not limited to: • Use Customer's EDR to quarantine/isolate an endpoint • Use an Identity Provider to block a user account • Reach out to Customer for approval to quarantine • Notify Customer of a confirmed incident <u>Customer Responsibility during the Rapid Quarantine Service:</u> • Ensure underlying EDR and Identity Provider service integrations remain in working order through periodic testing with CI • Un-isolating or un-blocking the quarantined assets once Customer has completed their remediation.

SERVICE REVIEWS (CI-MDR)	LUMIFI will coordinate with Customer during onboarding and schedule a cadence and duration for periodic service reviews. LUMIFI and Customer will use these scheduled meetings to discuss the service LUMIFI is providing, including discussing Customer's environment, the risks and trends LUMIFI has seen both in Customer's network and the wider threat landscape, and any Customer environment or contact changes.
XDR ALERTS (CI-MDR)	LUMIFI utilizes proprietary detections over log or alert streams to provide a better service that identifies and focuses on threats. These detections will show up as investigations or alerts alongside Customer's security product integrations. Customers can request custom detections. LUMIFI will prioritize these and undertake good faith efforts to complete them in a timely manner. LUMIFI may not complete all requests depending on circumstances such as Customer product licensing, data limitations, or other limitations, but will make commercially reasonable, good faith efforts to identify Customer risk while balancing false positives & negatives. Customer may escalate these by purchasing additional professional services, charged and governed in a separate Scope of Work.
DASHBOARDS & PORTALS	LUMIFI Customers have access to the Lumifi Cyber Customer Portal. The Customer Portal provides a central place to review information about the services provided and access 3rd party tooling. Information available across the Customer Portal and 3rd party tooling includes: • Details on SOC investigations • Ability to search through alerts and data for in scope log sources • Data ingest dashboards • CVI data and dashboards if CVI is part of Customer's service subscription • Routine reporting • Customer has the ability to download and save monthly reports to support reporting and auditing as needed
SUPPORT REQUEST	Customer can submit a support request through approved LUMIFI communication channels inquiring about a support or cybersecurity concern. Example requests include: • A question about an alert or concerning activity seen in Customer's environment • Secure environment configurations • Security product recommendations based on LUMIFI's experience • Assistance in working with other security providers, such as an EDR vendor LUMIFI will make commercially reasonable, good faith efforts to provide the information requested. Requests will be prioritized and worked as LUMIFI resources allow, and complex or urgent requests may require a separate Scope of Work that may carry an additional fee.
CONTINUOUS VULNERABILITY IDENTIFICATION (CI-CVI)	LUMIFI will configure scans to automatically conduct internal network vulnerability scans at Customer-defined frequencies and scan targets. The scans will identify insecure configurations, open ports and services, vulnerable software/service versions, and missing patches that could lead to network exploitation. Reports and dashboards are made available via the Customer Portal. Reports include: • Steps to eliminate each vulnerability • Risk via CVSS scores to allow prioritization of remediation efforts

LOG RETENTION (CI-LR)	LUMIFI will store, hash, and encrypt the in-scope logs throughout the lifetime of the service. Customer can submit a request to LUMIFI support containing the log, source, and timeframe they want logs from. LUMIFI will then pull the logs according to the request & time zone on record and securely transfer the requested logs via LUMIFI's file share. Up to 5 data requests and up to 10% of total stored data can be requested per year. More requests may be subject to a data or professional services fee at LUMIFI's discretion. At any time in the 60-day period following the expiration or earlier termination of the contract term, LUMIFI will, at Customer's request, transfer stored data to Customer at Customer's expense pursuant to a mutually agreed upon methodology. Customer data remaining on LUMIFI's systems following such 60-day period shall be subject to deletion, at LUMIFI's sole discretion, pursuant to LUMIFI's then current data retention policy. <u>Customer Responsibility during the lifetime of the Log Retention service:</u> • Continue successfully forwarding the logs according to LUMIFI's deployment documentation and initial activation • Notify LUMIFI if the log source, source IP, or time zone of the logs have changed • Notify LUMIFI if additional log sources are added, in-line with the initial deployment actions

INCIDENT CLASSIFICATION FOR LUMIFI CYBER MDR

INCIDENT SEVERITY	DESCRIPTION
URGENT	An urgent priority security incident is an event or set of events that is believed to present a serious and immediate risk to Customer's environment. LUMIFI will contact Customer (contact on file) via phone and email to attempt resolution and execute any Rapid Quarantine actions agreed in mutually agreed upon Playbook(s). Examples of urgent priority security incidents include, but are not limited to: • Suspected account compromise with account misuse observed • Customer security device has alerted LUMIFI to a likely compromise that has been verified using other MDR data/tools with no evidence the security device has mitigated the incident • Suspected malware infection with evidence of immediate business impact • Communications observed with a suspected malicious host with evidence of data exfiltration or immediate business impact • Regulated data seen unencrypted going to an external destination
HIGH	A high priority security incident is an event or set of events that is believed to present a risk to Customer's environment. LUMIFI will contact Customer (contact on file) via phone and email to attempt resolution and execute any Rapid Quarantine actions agreed in mutually agreed upon Playbook(s). Examples of high priority security incidents include, but are not limited to: • Suspected or potential account compromise with no misuse observed • Suspected malware infection with evidence of malware spreading but no evidence of immediate business impact • Suspected or potential system compromise with no evidence of misuse • Regulated data seen unencrypted between two internal hosts
MEDIUM	A medium priority security incident is an event or set of events that may be a risk to Customer's network environment and may inform future Customer actions. LUMIFI will contact Customer (contact on file) via email to attempt resolution. Examples of medium priority security incidents include, but are not limited to: • Attempted account compromise with no evidence of success • Suspected malware infection with no evidence of malware spread or immediate business impact
LOW	A low priority security incident is an event or set of events that is not believed to represent a risk to Customer's network environment but does warrant immediate awareness and investigation. LUMIFI will contact Customer (contact on file) via email to attempt resolution. Examples of low priority security incidents include, but are not limited to: • Potentially unwanted program observed • Other issue that is not an immediate security threat observed

SERVICE LEVEL AGREEMENT

LUMIFI PRODUCT	DESCRIPTION	SERVICE LEVEL	SLA CREDIT

LUMIFI CYBER PLATFORM ***(CI-P)***	COLLECT, NORMALIZE, STORE, TRANSMIT, AND RETAIN IN-SCOPE SECURITY DATA	99.9% UPTIME IN A FOR THE COLLECTOR WHILE CLIENT NETWORK IS FUNCTIONAL	2% OF MONTHLY FEE
	MAINTENANCE OF LUMIFI COLLECTOR	REPLACEMENT DEVICES SHIPPED WITHIN 3 BUSINESS DAYS OF FAILURE	2% OF MONTHLY FEE
LUMIFI CYBER VIRTUAL SENSOR ***(CI-P-VM)***	MAINTENANCE OF SENSOR	REPLACEMENT VIRTUAL SENSOR IMAGE PROVIDED WITHIN 1 BUSINESS DAY OF FAILURE	2% OF MONTHLY FEE
LUMIFI CYBER LINUX SERVER SENSOR ***(CI-P-SENSOR)***	MAINTENANCE OF SERVER SENSOR	REPLACEMENT LINUX SERVER SENSOR SOFTWARE AGENT PROVIDED WITHIN 1 BUSINESS DAY OF FAILURE	2% OF MONTHLY FEE
MANAGED DETECTION AND RESPONSE ***(CI-MDR)***	EVALUATE ELEVATED SECURITY CASES AND DETERMINE IF THEY ARE FALSE POSITIVES OR ACTUAL INCIDENTS	99% OF CASES ESCALATED TO ANALYST FOR REVIEW IN A GIVEN MONTH EVALUATED WITHIN 90 MINUTES	2% OF MONTHLY FEE
	INCIDENT REPORTING	99% OF CONFIRMED INCIDENTS IN A GIVEN MONTH REPORTED TO CUSTOMER WITHIN 30 MINUTES OF CONFIRMATION	2% OF MONTHLY FEE
CONTINUOUS VULNERABILITY IDENTIFICATION ***(CI-CVI)***	SCHEDULED VULNERABILITY SCANNING OF CUSTOMER NETWORK; REPORT UPLOAD OF SCAN RESULTS	AS VULNERABILITY SCANS COMPLETE, REPORT DATA UPLOADED TO CUSTOMER PORTAL OR DELIVERED TO CUSTOMER WITHIN 48 HOURS OF SCAN COMPLETION	2% OF MONTHLY FEE

1. *SERVICE LEVEL AGREEMENTS ONLY APPLY TO PRODUCTS & SERVICES IN **GENERAL AVAILABILITY**. ALPHA AND BETA PRODUCTS & SERVICES ARE NOT SUBJECT TO THIS SLA. PLEASE SEE PAGE 1 FOR A LIST OF PRODUCTS & SERVICES AND THEIR COMMERCIAL AVAILABILITY STATUS.*

VIRTUAL SENSOR HYPERVISOR SPECIFICATIONS

Maximum Throughput in Gigabits/second	Reserved Virtual Cores	Reserved RAM	Reserved SSD space in Gigabytes
10	24	64	512
1	12	32	128
.5	8	16	128
.2	4	8	128

Stated specifications support the corresponding maximum network traffic inspection throughput. Performance may vary depending on your environment configuration and other variables.