# Lightstream Managed Security Services
# Technical Service Description

## Managed Firewall – Fortinet

# Table of Contents

# 1 Purpose of this document

The purpose of this document is to provide detailed technical descriptions services and procedures of the Lightstream Managed Security Services powered by ON2IT for the Managed Firewall (Fortinet) managed security service.

# 2 Definitions

A list of definitions is provided in Appendix B.

# 3 Stakeholders

The following Service Provider(s) and Customer(s) will be used as the basis of the Managed Security Services and represent the primary stakeholders associated with the services provided hereunder:

Service Provider: Lightstream Managed Security Services powered by ON2IT ("Provider"), further denoted in this document as Lightstream.

Customer(s): denoted in this document as Customer

# 4 Services Summary

The Lightstream mSOC™ cloud-delivered solution enables the outsourcing of all operational end-to-end cybersecurity management, including detection, remediation, prevention, and compliance. The Lightstream Security Operations Center becomes the customer's 24x7 SOC, strengthening security operations with the addition of 24x7 threat monitoring and automated response skills and resources.

## 4.1 The Lightstream mSOC™ solution

The Lightstream mSOC™ Security Operations Center Platform integrates comprehensive security technologies, including:

- Orchestration and automation
- Customer dashboard and communications portal
- EventFlow™ intelligent threat management
- Automated, dynamic playbooks
- Policy management

Next-generation firewalls, endpoint and cloud-based technologies in your network provide basic detection functions and generate events, alarms, and alerts to the mSOC™ Portal, the Lightstream platform enriches, correlates, and filters every single event. We actively work with you to develop network microsegments based on Zero Trust principles. This approach provides necessary insight into the criticality of your data, services and applications and drives the prioritization of our actions.

## 4.2 Managed Detection and Response (MDR)

As security devices and cloud applications feed their configuration data and alerts to the Lightstream mSOC™ Portal, every event is enriched, correlated, and filtered by our Zero Trust Contextualization Engine™.

By enriching, correlating, and filtering every alert through Lightstream's threat intelligence, coupled with knowledge about the customer's business environment and processes, the number of potentially harmful events is significantly reduced. The data analytics and machine learning techniques embedded in the mSOC™ Portal automate alert triage, ensuring Lightstream specialists focus on the critical events that matter most.

Lightstream's countermeasure playbooks automate responses to most known and unknown exploits and vulnerabilities and are improved with every SOC analyst action. As needed, our SOC analysts works with customers to implement short term remediation actions, such as blocking IP-ranges, shutting down hardware, patching software, or re-imaging machines.

## 4.3 Managed Prevention and Compliance (MPC)

Successful detection and remediation programs demand perfectly operating cyber defense technologies. Misconfigurations, device overload and outdated systems are common and can cripple cyber defense. Lightstream's Managed Prevention and Compliance Services manage and optimize customer security environments.

If procured, Lightstream maintains policies and signatures to ensure accessibility, security, and regulatory compliance. Outsourcing this challenge allows IT staffs to focus on important core business issues. We proactively investigate your infrastructure and hunt for weaknesses, errors, and vulnerabilities. When we find potential problems, we provide real-time Service Advisories complete with problem identification and recommended resolutions. With the addition of Managed Prevention and Compliance services, Lightstream executes policy management and updates on behalf of the customer, implementing all preventative and countermeasures for the managed devices.

## 4.4 Features at a glance

| Feature | MDR | MPC |
|---|:---:|:---:|
| mSOC™ Portal | ✓ | ✓ |
| 24x7 support | ✓ | ✓ |
| Zero Trust Contextualization Engine™ | ✓ | ✓ |
| Indicators of Good Analysis | ✓ | ✓ |
| Indicators of Compromise Analysis and Correlation | ✓ | ✓ |
| Remote Threat Support | ✓ | ✓ |
| Security Event Management | ✓ | ✓ |
| Security Information Management | ✓ | ✓ |
| Compliance Reporting | ✓ | ✓ |
| Periodic Analysis of Configuration | | ✓ |
| Service Delivery Manager | | ✓ |
| Unlimited Policy and Configuration Changes | | ✓ |
| Risk Assessment on All Changes | | ✓ |
| Firmware Upgrades | | ✓ |
| Incident and Problem Management | | ✓ |

## 4.5 Managed Fortinet Firewall Service Scope

| mSOC with Lightstream Zero Trust Automation & Orchestration Lightstream Cyber Incident Response Team (CIRT) | |
|---|---|
| **Managed Detection and Response (MDR)** | **Managed Prevention and Compliance (MPC)** |
| Automation & Orchestration Platform | Availability Monitoring & Backup |
| Threat Event Enrichment, Analysis & Correlation | Operational & Capacity Management |
| Incident Monitoring, Alerting & RCA | Updates & Upgrades |
| Remote Breach Support | Policy Compliance & Best Practice Validation |
| Security Dashboard | Device & Policy Configuration Change Management |
| Management Compliance Reporting | Automated Rules of Engagement |
| | Policy Topology Reporting |

# 5 Managed Detection and Response (MDR)

This chapter describes the key activities and features included in Lightstream's MDR services.

## 5.1 Zero Trust Contextualization Engine™

The Zero Trust Contextualization Engine™ is an engine that is fully embedded into the mSOC™ Portal which provides context to each event processed by Eventflow™. This context is provided by adding the business requirements, regulatory compliance frameworks, and information such as Zero Trust microsegments and associated compliance tags created during the setup and operations phases to the information available about the monitored environment(s). Context is added through the enrichment of the security events and the impact of events is constantly re-evaluated to allow for a continuous impact assessment of each security incident reported. Information that is taken into consideration includes:

- Which Zero Trust segments are available
- Which compliance frameworks are applicable to the Zero Trust segment (PCI-DSS/ISO/NEN/etc.); CIA rating of the data in the Zero Trust segment
- Primary and secondary escalation contacts
- Escalation methods (email, text messages, phone calls)
- Customer internal data classifications
- Customer internal security requirements
- Data type(s) (for example: PII, IP, patient data, personnel data, etc.)

Enrichment and correlation of events is done using a variety of different sources and methods, including but not limited to:

- EDL (external dynamic lists), both in-house maintained as externally sourced
- Threat intelligence feeds
- Sandbox environments
- External MISP (malware information sharing platform) feeds
- Other sensors within the customer network

## 5.2 Indicators of Good Analysis

To ensure 100% evaluation of all security events, Lightstream begins with an Indicators of Good (IoG) analysis. The principle behind this analysis is that automatically processing events identified as "good", allows us to focus on the residue as unknown or "bad". Traditional SIEM-based approaches, in contrast, highlight only known threats or Indicators of Compromise, however, the IoG process ensures no known or unknown bad events operate under the radar. Our automated process is driven by Eventflow™, a methodology based on Lightstream's best practices and experience serving as the security conscience across our clients.

## 5.3 IoC Threat Analysis and Correlation

Analysis occurs from the Lightstream SOC by our certified specialists. Malicious or unknown events (possible "indicators of compromise") will be logged as a ticket and, wherever possible, automatically mitigated. Lightstream uses various sources to determine the criticality and urgency of events and priority and action depends largely on the CIA value assigned by the client. If Lightstream suspects a breach in the client network, we will contact the appropriate client resource(s) with an initial discovery report and advice about subsequent steps. All tickets can be viewed and followed in real-time via the mSOC™ Portal, and Lightstream logs all client and third-party communications regarding each ticket.

## 5.4 Alerting

Once Lightstream triages and assigns a priority to an event, we engage with the customer to mitigate the event or provide guidance regarding the root cause of the event and whether the event was legitimate. The method of alerting can be customized as part of the operational model.

## 5.5 Incident Management

Incident management concerns both security and continuity related incidents and is the process of registering, allocating and solving disruptions in normal operations of the system. The process ensures the quickest and best possible resolution of incidents. The process describes how incidents and changes are registered, prioritized, and resolved. Disruptions can be reported by Customer as well as by Lightstream. Prioritization depends on the impact and urgency of the disruption and whether there is an alternative available.

The purpose of the process is to restore the expected service levels after unscheduled interruptions of the services provided to limit their effect on business continuity.

With regard to Incident Management, the following steps are defined:
- Registering a ticket by mSOC™ Portal, telephone, or email.
- The priority matrix is detailed in the Service Level Objectives (SLO). The incident must be accompanied by at least the following data:
    - Affected service
    - Priority
    - Description of the issue and possible cause
    - Device/asset (a serial number or location of the device)
    - Point of contact (telephone, e-mail address).
- Authorization and validation of the ticket applicant.
    - Lightstream validates the authorization of the initiator
    - Lightstream may further validate/verify the authorization
    - Based on this assessment, the incident is approved or rejected, and Customer is informed by Lightstream

- Lightstream assesses the ticket and provides an answer, implements a solution or workaround. Lightstream might ask Customer for additional information or data/logging, per email or phone.
- Lightstream performs the necessary tests and provides technical feedback
- Customer concludes whether the incident is solved. Both parties can propose to close the call, however, Lightstream makes the final decision
- Closed tickets can be reopened by Customer for any reason deemed necessary.

In principle, Customer determines the priority of an incident when it is reported in accordance with the SLO. The prioritization of a ticket can be re-evaluated after the ticket has been closed. Lightstream may decide to raise or downgrade a ticket, in close alignment with Customer.

RACI TABLE:

| Step | Description | MSSP | Customer |
|------|-------------|------|----------|
| 1 | Register a ticket via mSOC™ Portal, e-mail or telephone with relevant information | CAR | AR |
| 2 | Authorization of the applicant and validation of the request | AR | CI |
| 3 | Classification and triage of the ticket | AR | CR |
| 4 | Implementing answer/solution/workaround | AR | I |
| 5 | Test and provide feedback with results | CI | AR |
| 6 | If solved, case complete, see step 8 | AR | I |
| 7 | If unsolved, evaluation and adjustment of solution or escalation | AR | I |
| 8 | Closing and evaluation of incident | A | IR |

Legend: (R)esponsible, (A)ccountable, (C)onsulted, (I)nformed

## 5.6 Remote Threat Support

The Lightstream platform automates detection and response actions to most threat incidents, stopping them in their tracks. When a suspected attack warrants further investigation or reporting, Lightstream completes a root cause analysis. Correlating different sources of information, the SOC specialist creates a holistic view of each event, identifying the root cause, involved systems and what the attacker accessed, along with an assessment of the data impacted.

## 5.7 Security Event Management

Lightstream's security automation and orchestration platform (SAOP) monitors, correlates, enriches, and runs events through "run books" to achieve highly automated decision making based on threat context and customer context. All relevant data including customer network topology is housed within the mSOC™ Portal, giving customers real-time access to all information regarding security management in their environment.

## 5.8 Security Information Management

Through the mSOC™ Portal, Lightstream provides trend analysis and highlights risks to the customer environment. The mSOC™ Portal offers real-time and historical insight into important key performance indicators (KPIs). The portal includes a complete and unlimited history of all tickets, changes, and incidents, and provides insight into KPIs such as time-to-respond, time-to-resolve, number of managed devices experiencing problems, uptime and more. Based on this information, monthly reports are created which include an executive summary and detailed information about issues, including which events led to an incident and the details of each event. Reporting for breaches and incidents is prepared separately, enabling the client to easily report both issues in the context of laws and regulations. This report is continuously being developed and contains:

- Total number of events seen; Number of blocked threats
- Number of threats that require human action
- Number of security breaches and history
- Number of security incidents and history

The reports are available on an unlimited basis on the mSOC™ Portal and are generated every first of the month. Using the management console, more information is available, such as:

- Detailed information about detected and blocked malware and exploits
- Licensing
- Endpoint health status
- Endpoint version information
- Most frequently attacked endpoints, processes, and users

For long term retention of the data, Lightstream recommends that log files are exported to an external system.

## 5.9 Compliance reporting

The mSOC™ Portal provides a wealth of information to assist in reporting compliance on most governance requirements, such as ISO27001, SOX, HIPAA and PCI-DSS. Lightstream will work with customer to assist in matching various governance requirements with the provided data.

# 6 Managed Prevention and Compliance (MPC)

This chapter describes the key activities and features included when MPC is added to the Lightstream services.

## 6.1 Change Management

The change management procedure ensures that changes in the settings and configuration of devices are conducted in a structured and controlled manner. The added value of this process is to ensure minimal operational disruptions and to prevent negative outcomes by conducting a risk analysis of a change prior to carrying out the change. An important prerequisite is to properly document, assess, prioritize, and plan each change. The change can be tested prior to implementation if necessary. After implementing the change, the changes will be documented, reported on, and evaluated.

A distinction is made between standard changes and non-standard changes (see appendix A). These changes differ in the priority assigned to the change and the agreed resolve time.

Content updates regarding resilience, filtering, and threats (such as signature updates, URL filter updates, etc) have the highest priority. To ensure reliability, availability and proper systems management, content updates are performed continuously and are not included in the change management procedure. All automatic updates of this content are properly tested and assessed prior to its release by the manufacturer and found to be reliable.

Both Customer and Lightstream can initiate changes in the configuration. Carrying out standard changes is included in the contract.

## 6.2 Standard Changes

The prioritization and result obligation as described in the SLO apply to standard changes. For additional details on standard changes, please refer to Appendix A.

Every change is logged as a ticket in the mSOC™ Portal. Every change-ticket consists of a functional and technical description. Lightstream can rely on Customer or a third party for functional tests. Lightstream will do everything possible to provide the required data within appropriate time.

## 6.3 Non-standard Changes

The prioritization and result obligation as described in the SLO apply to standard changes. Non-standard changes, in the context of this document are all changes not included in section 6.2. For additional details on non-standard changes, please refer to Appendix A.

Every change is logged as a ticket in the mSOC™ Portal. Every change-ticket consists of a functional and technical description. Lightstream will rely on Customer or a third party for functional tests. Lightstream will, in any situation, do everything possible to provide the required data within appropriate time.

RACI TABLE:

| Step | Description | MSSP | Customer |
|------|-------------|------|----------|
| 1 | Register a ticket via mSOC™ Portal, e-mail or telephone with relevant information | CAR | AR |
| 2 | Authorization of the applicant and validation of the request | AR | CI |
| 3 | Classification and triage of the ticket | AR | CR |
| 4 | Implementing answer/solution/workaround | AR | I |
| 5 | Test and provide feedback with results | CI | AR |
| 6 | If solved, case complete, see step 8 | AR | I |
| 7 | If unsolved, evaluation and adjustment of solution or escalation | AR | I |
| 8 | Closing and evaluation of incident | A | IR |

Legend: (R)esponsible, (A)ccountable, (C)onsulted, (I)nformed

## 6.4 Root Cause Analysis Report

At the request of Customer, Lightstream will conduct a Root Cause Analysis (RCA) for disruptions in which Lightstream services are (or might be) involved. The RCA will include a detailed factual report of the events, supplemented with observations and conclusions. Lightstream will do its best to provide a (draft) RCA within 1 month.

## 6.5 Problem Management

Problem Management seeks to minimize the adverse impact of incidents by preventing incidents from happening. For incidents that have already occurred, the Problem Management process is designed to prevent these incidents from happening again.

When a problem occurs, the following generic steps are followed:
- Identify a potential Problem, including proper prioritization
- Systematic investigation, resulting in a Root Cause Analysis
- Identification of change(s) needed to resolve the Problem
- Once changes have been implemented, verify that the Problem has been resolved. Verification must be done by both Lightstream and Customer
- Problem closure

To raise proper attention on problems, Lightstream may raise a Security Improvement Advisory (SIA). Service Delivery Management discusses any SIA's submitted by Lightstream to the customer to proactively drive resolution.

## 6.6 Release, Availability and Configuration Management

### 6.6.1 (Dynamic) Content Updates

The managed assets will be configured to automatically download and install updates. This includes:
- Application database updates

- Anti-virus database updates
- Threat database updates
- URL database updates
- Dynamic URL filtering

All updates require an active internet connection. Some updates require data to be sent to cloud services unless Customer explicitly requested not to allow data to be sent to cloud services. In this case, Customer might not be able to use the offered services to the fullest extent.

## 6.6.2 Recommended Software Versions

At regular intervals, Lightstream will determine the recommended software version for the firmware/operating system of the managed devices. Lightstream performs stability and quality tests of new firmware released by the supplier to obtain a clear and complete picture of the stability of the firmware. The final recommended software version may depend on the customer specific situation. As soon as there is a change in the recommended software version for Customer, Lightstream will notify Customer and will suggest an upgrade. Lightstream will report this as a change.

When implementing firmware upgrades, Lightstream makes the following distinction in terms of necessary and priority:
- **Bleeding Edge Release**: Software release category. Just released by vendor, no (or very little) testing was performed, and is not recommended for any customer production environment. Lightstream aims to start testing within 14 days of release. Bleeding Edge Releases are not supported by Lightstream, and not recommended by Lightstream. SLO becomes void.
- **Latest Feature Release**: Software release category. Release - usually "late" in the latest major train of software - with focus on latest new features as released by vendor. Supported by Lightstream MSS. Recommended for all customers that desire maximum functionality.
- **Legacy Release**: Software release category. Release still in use in customer environments and still eligible for vendor support. Supported by Lightstream MSS, not recommended by Lightstream MSS unless demonstrable use case warrants it.
- **Stable Release**: Software release category. Release focused on stability and long-term support. Supported by Lightstream MSS. Recommended for managed customers that desire maximum stability.

Firmware upgrades are always implemented in consultation. However, Customer is obliged to give permission for the upgrade within one month of being notified by Lightstream.

Together with Customer, Lightstream will schedule an upgrade at a suitable time, stating the impact and any downtime. After completion of the upgrade, Lightstream will perform of basic checks (are the devices available, can any traffic be observed, etc). Customer is expected to perform functional tests to verify that the upgrade was installed satisfactorily, and the intended result has been achieved. To coordinate the update, customers must be reachable (preferably by telephone) at the time of the firmware upgrade and upon completion. Customer is not expected to be present on site unless this is necessary to perform tests or to identify any problems as a result of the firmware upgrade.

### 6.6.3 Process For A Single Device

RACI TABLE:

| Step | Description | MSSP | Customer |
|------|-------------|------|----------|
| 1 | Starting firmware upgrade, reboot device | AR | CI |
| 2 | Waiting for the device to be back online, performing basic tests | AR | CI |
| 3 | If upgrade successful, inform customer | AR | I |
| 4 | Perform functional testing | CI | AR |
| 5 | Troubleshooting in case of issues, perform rollback if unrecoverable | AR | CIR |
| 6 | Closing and evaluation of incident | A | IR |

Legend: (R)esponsible, (A)ccountable, (C)onsulted, (I)nformed

### 6.6.4 Process For A Cluster

RACI TABLE:

| Step | Description | MSSP | Customer |
|------|-------------|------|----------|
| 1 | Starting firmware upgrade on secondary device, reboot secondary device | AR | CI |
| 2 | Waiting for the secondary device to be back online, performing basic tests | AR | CI |
| 3 | Perform failover from primary to secondary device | AR | CI |
| 4 | Starting firmware upgrade on primary device, reboot secondary device | AR | CI |
| 5 | Waiting for the secondary device to be back online, performing basic tests | AR | CI |
| 6 | If upgrade successful, inform customer | AR | I |
| 7 | Perform functional testing | CI | AR |
| 8 | Troubleshooting in case of issues, perform rollback if unrecoverable | AR | CIR |
| 9 | Closing and evaluation of incident | A | IR |

Legend: (R)esponsible, (A)ccountable, (C)onsulted, (I)nformed

### 6.6.5 Testing Methods

Upon the release of a new firmware version, Lightstream will install the new version on testing systems to confirm that previous features used continue to function properly. Lightstream will document this upgrade process noting any issues or exceptional situations so that these are managed during the further roll-out or reported to the supplier. After a positive initial assessment of stability and functionality, Lightstream will select customers to form a diverse pilot group for initial installations of the upgrade in their environment. (Pilot group customers have explicitly stated their interest in early adoption of the latest firmware versions.) These early installations allow Lightstream to further confirm functionality and ensure stability.

### 6.6.6 Unsupported Firmware Versions

It is possible that new features are available in new firmware versions which have not been sufficiently tested by Lightstream and are therefore not yet on the list of recommended software versions. If the customer situation requires, Lightstream will provide Customer with this firmware version. Lightstream will try to perform a quality check of the relevant firmware version but may not be able to perform the same extensive check as with a regular firmware upgrade.

## 6.7 Backups

A full audit trail of all actions and revision history is available in the management portal.

## 6.8 Health Monitoring

Lightstream will closely and continuously monitor the status of the platform and managed endpoints. Lightstream monitors the following aspects, among others:

- Availability of the management portal and platform
- Hardware defects
- Unexpected reboots
- Up-to-date version of dynamic (anti-virus, URL filtering, vulnerabilities, threats) and firmware updates; Internal temperature
- External temperature
- Operation and speed of the fans; Voltage stability on power rails; Other alarm conditions

Lightstream also verifies that the configuration of the platform meets the set requirements to prevent any unsafe ruleset. If our systems detect an alarm or off-nominal condition, a ticket will be generated at Lightstream.

## 6.9 Static Analysis On High-Risk Rules

Lightstream carries out a daily static analysis on the latest device configuration to automatically detect high risk rules in accordance with best practices. When a high-risk rule is detected, a ticket will be automatically generated to correct the high-risk rule.

## 6.10 Availability

Lightstream confirms platform availability multiple times per minute. If the platform is unreachable for 15 consecutive minutes, a ticket will be generated, and analysis of the cause will be conducted. Customer will be informed of the analysis result. External factors like an internet outage, infrastructural outages as a result of Customer error or power outage are excluded from the availability guarantee Lightstream provides.

## 6.11 Accountability and Verifiability

Lightstream logs every change with a ticket. All tickets are available in real-time through the mSOC™ Portal. Every change will consist of a functional description and a description of the changed policies and configurations. All communication (through the mSOC™ Portal, via e-mail or telephone between Lightstream and Customer or any third parties) with regards to the change is logged in the ticket and is available for an unlimited amount of time.

## 6.12 Risk Analysis

For each change, Lightstream conducts a risk analysis. If Lightstream believes that the risk of the change is 'high' or 'medium', Lightstream will explain this in the ticket and will, where possible, advise on how to mitigate this risk. If possible and/or known, Lightstream will also provide an alternative that entails a lower risk. In the event of such changes, Lightstream will offer "sound and well-founded resistance". If the Customer insists on implementing the change, Lightstream will require final and written confirmation from Customer.

## 6.13 Reporting and Monitoring

### 6.13.1 On-box Logging

The managed appliances have a large diversity of log files from which useful information can be distilled. We call this "on-box". Lightstream can generate multiple reports in accordance with the functional requirement of Customer. These reports can be generated in several file formats, including PDF and CSV. The generated reports can be e-mailed to one or multiple contacts within the Customer organization, automatically.

Some examples of reports:

- Visited URL's per user
- Bandwidth usage per application and/or user
- Real-time bandwidth usage per application and/or user
- Detected vulnerabilities
- Detected viruses, malware and trojans

The retention of these logs depends on the amount of storage allocated on the device. Customer can request one or multiple read-only accounts on the managed appliances, enabling Customer to review all configurations and generate custom reporting based on requirements. Generating reports per user can be a privacy violation. Customer is responsible for the correct submission of such requests in accordance with procedures regarding the request of privacy sensitive information.

### 6.13.2 Off-box Logging

If Customer wishes to use an external reporting or monitoring tool, guaranteed log file retention (e.g. an off-box copy) of the log files, Lightstream offers several options. The managed device supports the following protocols for this goal:

- Export through SCP (FTP over SSH)
- Export through FTP
- SNMP
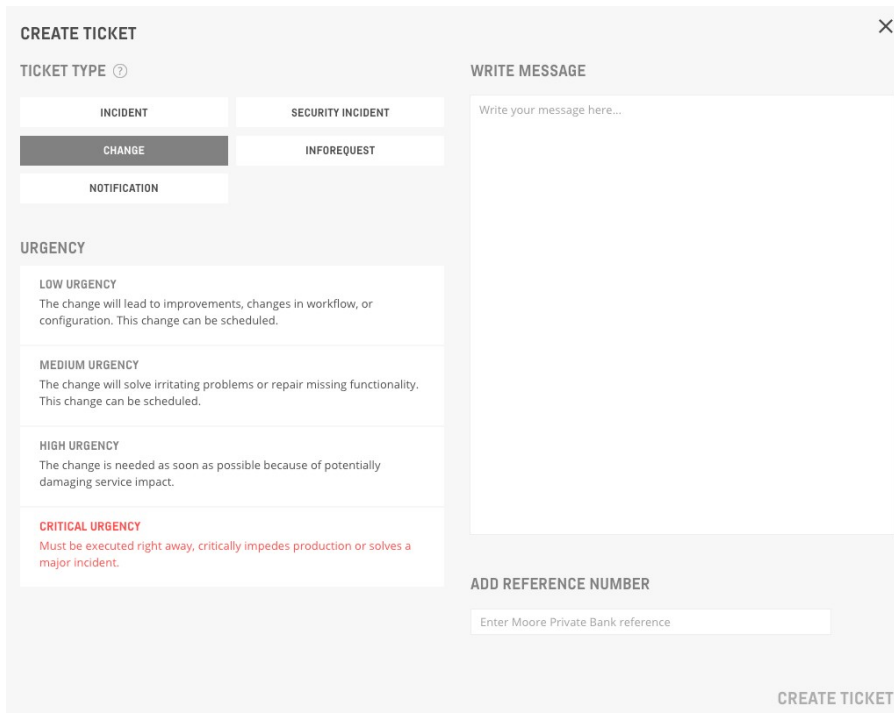- Netflow
- Syslog
- E-mail

### 6.13.3 Trend Analysis

The on-box reporting module enables Customer to conduct trend analyses. This functionality enables Customer to easily detect changes in trends in, among others, load, use of certain websites, applications, bandwidth, users, or IP-addresses.

## 7 Communication and Support

To promote clear communication, Customer will appoint one or more designated contact persons at an operational level (list available in mSOC™ Portal). Customer can request an adjustment to the authorization matrix. Any such changes will be proposed for approval to employees of Customer with the proper authorization. Time to Respond as specified in the priority matrix is guaranteed on the basis of the set priority level. For a priority 1 or priority 2 incident, Customer must immediately contact the Lightstream SOC by telephone and must be available 24/7. The Lightstream Managed Security Services Desk offers secondary and tertiary support to Customer.

## 7.1 mSOC™ Portal

Via the mSOC™ Portal, Customer has a real-time insight into their security status, as well as the status of open or closed tickets, the agreed SLA, the time to respond, the Authorization Matrix, key performance indicators and an overview of threats and available Management Reports. The applicable mSOC™ Portal web-address is https://portal.lightstreamsecurity.io. Customer can also use self-service options in the mSOC™ Portal, such as generating or approving new tickets, closing tickets, and adjusting the priority of tickets. The mSOC™ Portal supports delegated management and cross-references, which enables the granting of certain authorizations to

**CREATE TICKET** ✕

**TICKET TYPE** ⓘ

| INCIDENT | SECURITY INCIDENT |
| CHANGE | INFOREQUEST |
| NOTIFICATION | |

**WRITE MESSAGE**

Write your message here…

**URGENCY**

**LOW URGENCY**
The change will lead to improvements, changes in workflow, or configuration. This change can be scheduled.

**MEDIUM URGENCY**
The change will solve irritating problems or repair missing functionality. This change can be scheduled.

**HIGH URGENCY**
The change is needed as soon as possible because of potentially damaging service impact.

**CRITICAL URGENCY**
Must be executed right away, critically impedes production or solves a major incident.

**ADD REFERENCE NUMBER**

Enter Moore Private Bank reference

**CREATE TICKET**

colleagues/relations/third parties in a well-structured manner.

## 7.2 E-mail

Questions, tickets or other requests can be submitted to the Lightstream SOC by email at soc@mss.lightstreamsecurity.io.

After sending an email to the SOC, a ticket is automatically generated. The SOC validates and prioritizes the ticket and starts processing it. If an email is received from an email address which has not been authorized, we will report this to an authorized employee of Customer for verification. We will only process such emails after the written approval of a person authorized by Customer. The progress and status of tickets submitted by email can be followed in real time via the mSOC™ Portal. If Customer responds by email to an already existing ticket, this response will automatically be appended to the ticket history. For priority 1 incidents, it is required that Customer follows up with a phone call to the Lightstream SOC. Every request reported by e-mail will initially be marked as priority 4.

## 7.3 Telephone

The Lightstream SOC can be reached by telephone for questions and generating a new ticket.

When Customer submits a new ticket, the Lightstream SOC will generate and complete this ticket, providing Customer with a ticket number. If Customer calls about an existing ticket, Customer should preferably state the ticket number when making the call, allowing Lightstream to quickly retrieve all information to assist Customer as quickly as possible.

A ticket number consists of a string of random alphanumeric characters. Any communication by phone is logged and appended by Lightstream to the ticket history. Ticket updates are also sent to the contact person by email.

## 7.4 On-site Support

Lightstream does not provide on-site support unless otherwise agreed between Customer and Lightstream. If Customer wants Lightstream to offer on-site support regardless, this must be coordinated by the Lightstream Account Manager or Customer Experience Manager. A fee may be charged for these activities.

## 7.5 Remote Support

If so desired and if indicated by Customer in a timely manner, Lightstream can offer remote support. This must be coordinated by the Lightstream Account Manager or Customer Experience Manager. A fee may be charged for these activities.

## 7.6 Escalation Procedure

If deemed necessary by Customer or by Lightstream, an escalation procedure can be initiated for any type of ticket (e.g. lack of progress, quality of solution, etc). To initiate an escalation procedure, Customer calls the Lightstream SOC and asks for an escalation, after which Customer receives a confirmation by email. Within the mSOC™ Portal, the relevant ticket will be given the status 'escalated'. The status of each 'escalated' ticket will be assessed daily and communicated to Customer.

### 7.6.1 First Level of Escalation

Role: Service Delivery Manager

E-mail address: security-sdm@mss.lightstreamsecurity.io

Phone: 24x7 Support Number

### 7.6.2 Second Level of Escalation

Role: Manager MSS

E-mail address: manager-mss@mss.lightstreamsecurity.io

Phone: 24x7 Support Number

# 8 Prerequisites

This service is applicable to the following hardware platforms:
- Fortinet Fortigate Firewalls

The customer must comply with the following prerequisites for this service:
- The procurement of required licenses and/or hardware covering the products that will be used in this engagement (If the licensing and/or hardware is not provided by Lightstream as part of the service offering)
- There shall be no 'pre-existing conditions' (e.g. customer network, application or endpoint problems that existed prior to implementation or withheld issues)
- A completed Lightstream SMS Managed Fortinet Firewall Onboarding Document

The following stakeholders are required to set up and deliver this service:
- Primary POC
- Network Architecture Team Leads
- Network Security Team Leads

- Security Team Leads
- Security Policy Team Leads

## 8.1 On-Premises Specific Requirements

If required, physical or virtual hardware, including servers, storage, and networking, must have been procured, installed, configured, and confirmed to be operational.

HTTPS connection (can be restricted to SOC IP address ranges) or IPSEC VPN ('always on') connection between customer and SOC, configured according to a mutually agreed configuration proposal.

# 9 Obligations of the Parties

## 9.1 Lightstream

Lightstream is responsible for the quality of the delivered Service, as detailed in this document. This includes:
- Providing the services described herein
- Providing service support by properly trained and certified staff, which are continuously trained and recertified
- Achieving response times in handling and resolving incidents, as defined below. Based on this, Lightstream will allocate an appropriate amount of personnel with adequate knowledge to offer the Service
- Appropriate and timely notification of Customer, providing relevant information which may impact the offered Service. Examples are scheduled maintenance, organizational policy changes and changes in processes and procedures.

## 9.2 Customer

Customer obligations and requirements in support of the service include:
- Proactive or on request of Lightstream, provide clear input to Lightstream for assessment of resolution of an incident or service request.
- Availability (24/7) of Customer representative(s) for Lightstream when resolving a P1 or P2 issue or troubleshooting an incident.
- Appropriate and timely notification, preferably three working days upfront, of scheduled maintenance within Customer systems which are deemed relevant for Lightstream to know.
- Keeping Lightstream informed on changes with respect to the Authorization Matrix.
- Notification of all relevant network and physical changes to the managed equipment (e.g. location changes).
- Adequate follow-up of any reported Security Improvement Advisories (SIAs) as reported in the monthly Management Reports.
- The customer already has installed and configured Palo Alto Networks Cortex XDR security infrastructure as detailed in the onboarding checklist.  If the customer is procuring Cortex XDR as a portion of the Lightstream services, the customer is expected to install and configure the licenses on the endpoint

Any change to the scope of work explicitly described in this service description sheet, and any associated additional fees, must be mutually agreed to in writing.

## 9.3 Reporting

Lightstream provides real-time data on the service provided, available to Customer, via the mSOC™ Portal. Additionally, on a monthly basis, Customer can obtain a Management Report. The Management Report is available for download within five working days after the end of each month. The mSOC™ Portal and management reports provide an overview of the quality of service delivered and an overview of tickets handled by Lightstream. If desired and on a

fair-use basis, Lightstream can provide additional ad-hoc custom reports, to be discussed with the Service Delivery Manager.

## 9.4 Performance

The following performance metrics are applicable to the services as described:

| Performance Indicator | Category | Timeframe | Performance Target[1] |
|---|---|---|---|
| Initial Response | P1 - P4 | 15 min | 90% |
| Workaround or Fix | P1 | 8 hours | 90% |
| Standard Change | P1 - P3 | 8 hours | 90% |
| Standard Change | P4 | In conjunction with customer | 90% |

For a description of the severity levels, see Appendix A.

# 10 Quality Management

## 10.1 ISO 9001:2015 and ISO/IEC 27001:2013

Lightstream Security Managed Services powered by ON2IT is both ISO 9001:2015 and ISO/IEC 27001:2013 certified. This means that our Quality Management System and our Information Security Management System meet the strict requirements of ISO.

## 10.2 Certifications and Partner Status

To ensure the best possible services and quality, all Lightstream engineers are continuously educated and (re)certified on the required levels for products in scope.

# 11 Complaint Handling

Any complaints can be submitted to Lightstream, following the Customer Complaint Procedure, which can be requested via info@security.ltstream.com. Lightstream's Customer Experience Manager will consult with Customer and will, where necessary, take measures to prevent any repetition. Each month, the Customer Experience Manager will report any complaints to the management of Lightstream.

# 12 Security and Data Locality

Lightstream takes pride in her security policies and strictly follows internal guidelines as well as ISO requirements.

## 12.1 Authorization and Access to Systems

Depending on the type of service provided, Lightstream may need access to systems which are under supervision and/or control of Customer.

## 12.2 Authorization and Access to the mSOC™ Portal

Customer has the responsibility to only allow authorized personnel on the mSOC™ Portal. The mSOC™ Portal is accessible with a unique, personal username and password. For additional security, Lightstream offers multi-factor authentication. Lightstream strongly advises Customer to enable this feature for access to the mSOC™ Portal.

## 12.3 Data Location and Backup

All data which is handled by Lightstream is stored in The Netherlands or the United States, depending on theater. All critical systems of Lightstream are redundant, in active-active or 2N-setup. Lightstream uses multiple availability zones (physical locations) for her servers and data storage.

## 12.4 Additional Security Measures

For customers with HQ locations in the European Union, data is processed and stored within The Netherlands. Lightstream offers their services in line with the EU General Data Protection Regulation (GDPR).  All other customers must request that locations within the European Union have all data processed and stored with The Netherlands.

## 12.5 Personnel

Role-based access policy is enabled for all Lightstream personnel, which means that all Lightstream personnel has 'need-to-know' access to only data which is deemed relevant for their function or role.

All Lightstream personnel are screened by an external screening agency: A pre-employment screening and, where applicable, an assessment of knowledge and skills is pursued.

If required by regulations, applicable Lightstream personnel is screened by appropriate governmental agencies.

Lightstream will not divulge personal information such as date of birth or cell phone number of personnel to Customer.

# Appendix A:  List of Standard and Non-Standard Changes

Lightstream distinguishes two types of changes, largely following ITIL principles.

## A.1 Standard Changes

A standard change is one of recurring nature, performed frequently and is relatively low risk. Standard changes are requested and performed often, and do not require a design or project management. A list of changes that Lightstream regards as "standard":

- Create, remove, or adjust access rules
- Create, remove, or adjust NAT rules
- Create, remove, or adjust URL profiles
- Create, remove, or adjust objects
- Create, remove, or adjust static routes
- Create, remove, or adjust application override policies
- Create, remove, or adjust IPSEC/IKE configuration
- Create, remove, or adjust basic interface configuration (IP, subnet, zone assignment)
- Create, remove, or adjust local users or user groups
- Create, remove, or adjust local reports
- Create, remove, or adjust DHCP server or relay settings
- Create, remove, or adjust local log forwarding

## A.2 Non-Standard Changes

A non-standard change is anything that does not fit into a standard change. Lightstream will try to perform non-standard changes in much the same way as standard changes where possible. However, in case Lightstream determines that a non-standard change will be too complex or high risk, Lightstream may require:

- A technical design, for example when a large restructuring/renumbering of the customer network needs to happen
- A project manager, for example when many stakeholders are involved
- On-site presence, for example a physical move of hardware

It is the responsibility of the customer to assign a local point of contact with technical and subject matter knowledge. An example of what Lightstream regards as "non-standard":

- Implementing dynamic routing (e.g. OSPF, BGP)
- Implement quality of service or policy based forwarding Implement IPv6 services
- Implement captive portal
- Implement client-to-site VPN
- Implementation of Zero Trust in a legacy network Perform a failover or firmware upgrade

# Appendix B:  Definitions

The following definitions may be referenced in this document:

- **Asset**: See managed object.
- **Authorization Matrix**: A list of personnel authorized to contact and their privileges.
  - Example: Handing in change requests, initiation of changes, creating incidents.
- **Backup**: A configuration backup of a managed device.
  - Example: An XML configuration ftle containing the backup of a managed device.
- **Best Practice Policy**: Set of procedures that are accepted or prescribed as being most effective, based on prior knowledge, common practice and company experience.
- **Bleeding Edge Release**: Software release category. Just released by vendor, no (or very little) testing was performed, and is not recommended for any customer production environment. Lightstream aims to start testing within 14 days of release. Bleeding Edge Releases are not supported by Lightstream, and not recommended by Lightstream. SLO becomes void.
- **Change**: The addition, modification, or removal of anything that affects the provided service or equipment according to the standard and non-standard change definitions.
  - Example: Policy change, configuring a new feature, etc.
- **CIA or CIA-triad**: Confidentiality, Integrity and Availability
- **Critical Business Impact Incident ("P1"):** Production application down or major malfunction resulting in a product inoperative condition.
  - Example: Users unable to reasonably perform their normal functions. The specific functionality is mission critical to the business and the situation is considered an emergency.
- **Critical impact security incident ("P1")**: An event where the attack was likely to have succeeded and exploitation is currently ongoing, causing critical damage to business assets, reputation, or information.
  - Example: Ransomware that is currently encrypting ftle shares.
- **Critical risk SIA**: A security improvement advisory that needs to be addressed immediately (within 1 day). If not addressed, severe adverse business impact is likely.
  - Example: Repeated and structural unavailability of points of contact at customer, leading to tickets (e.g. security incidents) to go unanswered and causing a security risk for customer.
- **Critical Urgency Change ("P1"):** Must be executed right away, critically impedes production or solves a major incident.
  - Example: An unplanned, urgent configuration change that denies outgoing traffic to stop a ransomware outbreak.
- **Diagnosis**: A stage in the incident and problem lifecycle. The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem.
- **Downtime**: The time when an IT service or other configuration item is not available during its agreed service time.
- **Escalation**: An activity that obtains additional resources when these are needed to meet service level targets or customer expectations. An escalation is triggered by following the escalation path as agreed between customer and Lightstream.
- **Event**: systematic output of our monitoring systems and underlying automated processes, which is assessed against a predefined ruleset to determine the significance. If determined to be of importance for further action because of a (potential) interruption of service or deterioration of the quality of ser- vice, these events are further analyzed and possibly followed up by a ticket. Not all events are visible or accessible to customer.
  - Example: Any "raw" event generated by a monitored security environment
- **Fix**: A fix is a measure to remove the impact of an incident or a problem by resolving the root cause.

- **High Business Impact Incident ("P2"):** Critical loss of service functionality or performance resulting in high numbers of users unable to perform their normal functions.
    - o Example: Major feature/product failure; inconvenient workaround or no workaround exists. The service is usable but severely limited.
- **High impact security incident ("P2"):** An event where the attack was likely to have succeeded, further exploitation is likely, and will mean damage to business assets, reputation, or information.
    - o Example: Malware was successfully installed on an endpoint and is currently communicating with a command and control server.
- **High risk SIA:** A security improvement advisory that needs to be addressed with high priority (within 1 week). If not addressed, could lead to serious business impact.
    - o Example: The inability or unwillingness of customer to facilitate timely maintenance windows for Lightstream to execute security updates in managed devices.
- **High Urgency Change ("P2"):** The change is needed as soon as possible because of potentially damaging service impact.
    - o Example: An unplanned change to allow traffic between two network segments for an urgent software upgrade.
- **Incident**: Incident management concerns both security and continuity related incidents and is the process of registering, allocating and solving disruptions in normal operations of the system.
- **Inforequest**: An information request is any question that does not involve a change or (security) incident.
    - o Example: For example, questions about product features or Lightstream services.
- **Initial response**: Acknowledgement of Incident, request for Change, Notification, Request for Information by providing a Ticket number, the name of the responsible engineer, actions to be taken and expected time for next status update.
- **Latest Feature Release**: Software release category. Release - usually the most recent software including new features as released by vendor. Supported by Lightstream MSS. Recommended for all customers that desire maximum functionality.
- **Legacy Release**: Software release category. Release still in use in customer environments and still eligible for vendor support. Supported by Lightstream MSS, not recommended by Lightstream MSS unless demonstrable use case warrants it.
- **Low business impact Incident ("P4"):** Minor loss of service functionality.
    - o Example: Usable performance degradation.
- **Low impact security incident ("P4"):** An event where no information was obtained and/or the attack was definitely blocked.
    - o Example: A port scan from the Internet to a public IP address which was blocked.
- **Low risk SIA**: A security improvement advisory that needs to be addressed with low priority (within 3 months).
- **Low Urgency Change ("P4"):** The change will lead to improvements, changes in workflow, or configuration. This change can be scheduled.
    - o Example: A planned configuration change that will result in better network convergence in event of a hardware failover.
- **Managed Object:** A device, service or platform which is managed by Lightstream for her customers.
    - o Example: A physical or logical (e.g. cloud) based firewall, an endpoint solution, a cloud management platform, etc.
- **Medium business Impact Incident ("P3"):** Moderate loss of service functionality or performance resulting in multiple users impacted in their normal functions.
    - o Example: Minor feature/product failure, convenient workaround exists/minor performance degradation/not impacting production.

- **Medium impact security incident ("P3"):** An event where no information was obtained and/or the attack appears to be blocked but follow up investigation is needed.
  - o Example: A virus that was delivered via e-mail but was blocked and quarantined upon execution, where the "why" question still has to be answered (e.g. why was it not blocked earlier).
- **Medium risk SIA:** A security improvement advisory that needs to be addressed with medium priority (within 1 month). If not addressed, the situation could lead to moderate business impact.
  - o Example: A lack of follow up to ruleset improvement suggestions such as cleaning up old objects or legacy rules, causing an increased risk surface to exist.
- **Medium Urgency Change ("P3"):** The change will solve irritating problems or repair missing functionality. This change can be scheduled.
  - o Example: A planned configuration change to allow traffic for a to be installed software platform.
- **Non-standard change**: A non-standard change is anything that is defined as a standard change.
  - o Example: Configuration of dynamic routing in a customer environment, a firmware or management software upgrade, etc.
- **Notification**: A notification ("heads up") to inform the receiving party of an impending event (e.g. maintenance).
  - o Example: Planned maintenance, planned fail over test, planned penetration test, etc.
- **Onboarding**: The predefined process, defined by Lightstream, to operationally enable the service at customer.
- **Onsite assistance**: Assistance offered by qualified staff of Lightstream at the location of customer.
- **Pending state**: Ticket is waiting for Lightstream action or response.
- **Planned Downtime**: Agreed time when an IT service will not be available.
  - o Example: Planned maintenance, a planned move of devices, etc.
- **Post-Mortem Analysis**: A Root Cause Analysis for Security Incidents / Exfiltrations.
- **Problem**: A cause of one or more incidents. By means of a Root Cause Analysis, the problem at hand is analyzed and a solution or workaround is defined. Problems can result in a Service Improvement Advisory, which is input for further discussion between customer and Lightstream.
- **Relevance**: Number between 0 and 100, 100 being highest, indicating the security relevance of a microsegment to the customer.
- **Remote assistance**: Remote assistance offered by qualified staff of Lightstream.
- **Replacement Unit**: Usually called FRU - Field Replaceable Unit, this concerns a physical hardware unit which is shipped to customer or replaced by Lightstream (depending on the applicable subscription of customer).
  - o Example: A physical firewall, a power supply, etc.
- **RMA**: The process of returning physical assets to Lightstream.
  - o Example: A defective device, or a device that is no longer needed is returned.
- **Root Cause**: The underlying, originating cause of an incident or problem.
- **Root Cause Analysis**: The activity of identifying the underlying, originating cause of an incident or problem. This process may result in a Root Cause Analysis report to document an event, identifying areas for improvement.
- **Scheduled State**: Ticket is on hold until a predetermined date and time (mutually agreed between customer and Lightstream).
- **Security Advisory**: See SIA.
- **Security Improvement Advisory**: Advice recommending actions to improve security and/or continuity. If not acted upon, Lightstream cannot be held liable for potential consequences.
- **Security Incident**: A Security Incident is an event that may indicate that an organization's systems or data have been compromised. A security incident may be automatically generated based on one or more events or created manually.

- Example: Observation of virus, ransomware, hacker, or behavior that indicates as such.
- **Security Operations Center (SOC)**: Team of certified security engineers, which takes in, analyzes, and solves continuity incidents, security incidents and performs customer requests.
- **Service**: The Service, as described in the Service Description and Procedures document, provided to the customer.
- **Service Hours**: 24x7
- **Service Level**: Measured and reported achievement against one or more service level targets