SOC Support Program & SLA Overview

Effective April 8, 2025

CyFlare's SOC Support Program goes beyond a traditional outsourced SOC provider by seamlessly integrating expert security professionals into your team. This collaborative approach ensures we understand your unique security needs and can proactively address potential threats. We're committed to safeguarding your systems, data, and services as our own. We'll empower your organization to continuously improve its security posture through ongoing monitoring, rapid incident response, and solution-tuning workshops.

Support Resource Layers:

Our higher-level support tier offers our SOC Analyst Team and a client-appointed contact to build a long-lasting relationship and become an extension of your team. Our analyst teams constantly work to identify, investigate detections, and alert your team of suspicious activity. We also provide deep technical expertise to assist with advanced incident response situations when needed.

Service Level Agreements:

Several solutions are supported across the CyFlare portfolio. The timetables below identify the applicable SLAs (agreements) and SLOs (objectives) for each scenario, such as tool-generated alarms, inbound client service requests, or client-reported security incidents. Unless explicitly stated under a separate agreement, the SLAs apply to all clients and solutions.

Understanding CyFlare's Service & Security Event Lifecycle

At CyFlare, we prioritize transparency and accuracy in how we measure and report our service performance. To help you better understand the different stages of a potential security event and how we evaluate our response times, we've outlined the key timestamps involved and how they contribute to our Service Levels.

Key Timestamps in the Security Event Lifecycle

1. **Raw Telemetry Event Occurrence**
   This timestamp marks the **true original occurrence** of a potential threat within your environment. It is generated by your systems and is **completely outside of CyFlare's control**. This reflects when the event actually happened, not when it was detected.
2. **Source Security Control Trigger of Detection(s)**
   At this point, your security technology (e.g., SIEM, EDR) has **processed the raw telemetry data** and identified it as something noteworthy. This is when an **alert or detection** is triggered, signaling that the event requires attention.
3. **CyFlare Ingestion of Detection**
   Here, the detection/alert is **ingested into CyFlare's SOC platform**. This timestamp marks when the **CyFlare SOC first sees the detection**, allowing our analysts to begin their investigation. This is a critical moment as it signals the beginning of the review process.

CyFlare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

P: +1 877-729-3527
E: sales@cyflare.com

4. **CyFlare Ticketing System Disposition**
   After CyFlare's SOC team reviews the case, if it's determined that the detection requires your attention, a **ticket is created in our customer-facing system**. This ensures that you are promptly informed of the issue with the relevant context and analysis provided.

How CyFlare Measures Service Performance

- **Service Mean Time to Disposition (Service MTTD)**
  This metric evaluates how quickly CyFlare responds to detections once they reach our system. This is the metric shared within ONE related to MTTD. It is calculated as:
  - **Service MTTD = Timestamp (4) - Timestamp (3)**
  - This reflects the time taken from when **CyFlare first ingests the detection** to when it is **either closed by our SOC** or **made visible to you via a ticket**. This measurement helps us track the efficiency of our SOC operations.

SOC SLA: Service MTTD

The following table outlines security event severity levels and the timeframe to review, acknowledge, and provide initial responses. This approach applies to any tool that may generate security alarms for SOC investigation and response.

Benefit	Advanced	Premiere
Critical (highest severity) • Priority incident that could cause severe or irreparable damage to the client's critical infrastructure and reputation • Results in root-level compromise of servers or infrastructure devices • Exploitation is typically easy to accomplish • A product is not functioning, and a viable workaround is not available	Up to 1 hour	Up to 30 minutes
High • Incident likely to result in demonstrable impact or potential for severe impact on client critical infrastructure and reputation • Vulnerability is difficult to exploit • Exploitation could result in elevated privileges	Up to 4 hours	Up to 2 hours

• Exploitation could result in significant data loss or downtime		
Medium • Incident or event that has the potential to cause a moderate impact on critical or non-critical infrastructure • Exploits or vulnerabilities that require escalated credentials • Vulnerabilities where exploitation provides limited access • Vulnerabilities that require manipulation of victims using social engineering tactics	Up to 12 hours	Up to 4 hours
Low (lowest severity) • For investigation purposes only against an IOC (Indicator of Compromise)	Info only	Info only
NOTE: Severity is determined based on the scoring or severity rating from the source tool.		

CyFlare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

P: +1 877-729-3527
E: sales@cyflare.com

Technical Operations SLO: Customer Request Response Time

Severity Level	Advanced	Premiere
Critical (highest severity) • The client reported security incidents (Insider threat, known incident, etc.) • A product is not functioning, and a viable workaround is unavailable, impacting critical systems.	Up to 4 Hours	Up to 1 hour
High • Product issue that is significantly impacting end-users or client infrastructure. Systems are accessible but degraded. • Sensor connectivity	Up to 1 Business Day	Up to 4 hours
Medium • Troubleshoot operational issues with agents affecting endpoints • Configuration changes • Agent connectivity/upgrade requests	Up to 2 Business Days	Up to 1 Business Day
Low (lowest severity) • Account & credential management • Implement data filter changes • Create feature requests for new integrations, parsers, and plugins with the vendor as needed.	Up to 5 Business Days	Up to 2 Business Days

CyFlare Security Inc.
950A Union Road, Suite 103
West Seneca, NY 14224

P: +1 877-729-3527
E: sales@cyflare.com

SLA Measures and Credits:

The following table identifies the credits for SLA violations and their measures.

Service	Definition	Measure	Credit
Incident Investigation & Response	CyFlare must respond to each detection of the deployed solution(s) raised within the table above for related managed security solutions. All monitored security solutions have the same SLA unless explicitly identified within the Customer SOW. Timeframes will be determined from when the detection notification is created to the timestamp of the SOC-generated ticket to the Customer or when the event is closed within the CyFlare ONE Platform.	97% attainment across the monthly service period	1/30th of the monthly service fee for each business day that the SLA is not met. Credit is not to exceed 50% of the monthly service fees.

Credit Payment:

Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to CyFlare of such failure. To receive a Service Level credit, the Customer must submit the notification of the Service Level failure to CyFlare within forty-five (45) days of such failure. CyFlare will review the request and respond to the Customer within thirty (30) days from the date of the request.

The total amount credited to a customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by the Customer for such Service. Except as otherwise expressly provided hereunder or in the Master Services Agreement, the previous Service credit(s) shall be the Customer's exclusive remedy for failure to meet or exceed the previous Service Levels.

If the Customer pays the Fees annually in advance, CyFlare shall pay the credits due to the Customer in one of the following methods:

- Credit is to be applied to the next applicable invoice for the annual fees or
- In the form of a check to be paid to Customer within thirty (30) days after request by Customer