SOC Support Program & SLA Overview

Effective October 2023

Two Organizations, One Security Team —

Your outsourced SOC provider cannot be a passive partner and must be as integrated as possible within your team to extract maximum value and minimize risk. Our trained staff members will treat your systems, data, and services as their own. Initial tickets raised to highlight indicators of compromise often lead to solution-tuning workshops and consultation by your SOC to help you identify possible visibility or defense gaps and assist with continuous improvement.

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. Tier 1 and Tier 2 analyst teams are constantly working to identify, investigate detections, and alert your team of suspicious activity and provide deep technical expertise to assist with advanced incident response situations when needed.

One Team	• SOC analyst • Client-appointed contacts
Tier 2	• Unlimited incident response • Incident summary reporting
Tier 1	• 24x7x365 detection monitoring • First line of defense

Service Level Agreements —

Across the CyFlare portfolio, there are several various solutions supported. The timetables below identify the applicable SLAs 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.

SOC SLA:

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

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

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

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 • Exploitation could result in significant data loss or downtime	Up to 4 hours	Up to 2 hours
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.		

Technical Operations SLO:

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	Up to 5 Business Days	Up to 2 Business Days

CyFlare Security Inc.
21 Goodway Drive, Suite A4
Rochester, NY 14623

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

• Create feature requests for new integrations, parsers, and plugins with the vendor as needed.		

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 the time the detection notification is created to the timestamp of the SOC-generated ticket to the Customer or 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