CYFLARE
The threat stops here.

SOC Support Program & SLA

Overview and Highlights

Effective October 2021

CYFLARE
The threat stops here.

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.

Effective October 2021

877.729.3527
www.cyflare.com
sales@cyflare.com

CYFLARE
The threat stops here.

SUPPORT LEVEL OPTIONS

The CyFlare SOC offers 3 tiers of support to best align with your needs.

Essential Level – Included in all managed security offerings. Provides an aggressive timeframe for incident alerting, and unlimited incident response.

Enhanced Level – Includes Essential Level support benefits with expedited response timeframes.

Premiere Level – Includes Enhanced Level support benefits along with a rapid response dedicated senior security expert, regular cyber security posture assessments, ans weekly security briefings.

Essential → Enhanced → Premiere

SUPPORT LEVEL BENEFIT COMPARISON MATRIX

Benefit	Essential	Enhanced	Premiere
24x7x365 Monitoring & Alerting	✓	✓	✓
Formal Onboarding Process & Support	✓	✓	✓
Solution architecture & deployment guidance	✓	✓	✓
Unlimited Incident Response	✓	✓	✓
Security solutions recommendations & guidance	✓	✓	✓
Daily / Weekly Security Reports (based on toolset)	✓	✓	✓
Threat Campaign SOC Advisory	✓	✓	✓
Formal Incident Summary	-	✓	✓
Expedited Response Times	-	✓	✓
Configuration change requests per month (i.e., ATH, New content generation, feature requests, Parser requests)	2	5	8

Effective October 2021

877.729.3527 www.cyflare.com sales@cyflare.com

CYFLARE
The threat stops here.

BENEFIT DETAILS

This section defines the specific details related to each program benefit. The benefits lists and descriptions are below.

24x7x365 Monitoring & Alerting – The CyFlare SOC will provide monitoring of security alerts for associated CyFlare managed tools. This monitoring will facilitate the detection of potential threats to client networks that require additional research and investigation.

Formal Onboarding Process & Support – CyFlare will provide a "Welcome Package" with the process of welcoming new clients into the SOC Services to ensure they understand the services available to them. The process will include all required information to establish integration to your CyFlare SOC.

Unlimited Incident Response — CyFlare provides unlimited incident responses based on alert discovery per CyFlare managed source tool.

Security Solutions Recommendations & Guidance — SOC analysts are available with recommendations and guidance as required.

Daily/Weekly Security Reports — CyFlare reporting is based on source tool capability and can be scheduled (i.e., hourly, daily, weekly, monthly).

Expedited Response Times — Are available depending on the support plan selection (See Support Matrix above).

Configuration Change Requests per Month — Change requests can be requested in custom detections, new content generation, parser requests dashboard, and reporting). The number of requests per month is associated with the support plan.

Formal Incident Summary — In the event of a security incident, the SOC will provide structured investigation and remediation recommendations. These will be summarized in an incident summary report or resolved via a ticket resolution.

Threat Campaign SOC Advisory — Mass communication from the SOC related to widespread or target threat campaigns that may impact many clients. These advisories typically break down the known indicators, potential targets ,and what the SOC is doing to address the drive to provide visibility and protection to subscribed clients.

877.729.3527 www.cyflare.com sales@cyflare.com

CYFLARE
The threat stops here.

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 alarm, inbound client service requests, or client reported security incidents. Unless explicitly stated under a separate agreement, the SLAs apply to all clients and solutions.

SECURITY EVENT (OUTBOUND) HANDLING TIMETABLE

The following table outlines security event severity levels and the associated timeframe to review, acknowledge, and provide initial responses. This approach applies to any tool that may generate security alarms for SOC investigation and response, including the Breach Detection Service (BDS), Alien Vault, Splunk, Sentinel One, Sophos Intercept-X, Proofpoint Essentials, Azure Sentinel, etc.

Benefit	Essential	Enhanced	Premiere
Severe (highest severity) ▪ Priority incident that could cause severe or irreparable damage to client 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 4 Hours	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 ▪ Exploitation could result in significant data loss or downtime	Up to 8 Hours	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 24 Hours	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	Info only

NOTE: Severity is determined based on the scoring or severity rating from the source tool.

Effective October 2021

SLO (INBOUND) REQUESTS

The following table identifies the time target and priority for Inbound Requests.

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

SLA MEASURES & CREDITS TABLE

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

Service	Definition	Measure	Credit
Incident Investigation & Response	CyFlare is obligated to respond to each detection raised by the deployed solution(s) 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

Effective October 2021

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 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

Effective October 2021