CEQUENCE SECURITY

DATASHEET

Cequence Managed Services

Introduction

Cequence Managed Services extends your security team's expertise with operational capabilities that enable them to keep up with the growing trend of cyberattacks that target application programming interfaces (APIs). The managed services offering is a perfect add-on service for customers who deploy the Cequence Unified API Protection (UAP) solution to protect their APIs. Cequence delivers this service through a world class team of cybersecurity experts that are proficient in managing tens of thousands of API attacks across the world's largest and most demanding Fortune 50 organizations.

Cequence Managed Services is made up of three subscription-based modules.

API Discovery and Risk Monitoring

API Discovery and Risk Monitoring Managed Service provides you with assistance in configuring and managing **API Spyder**, an API attack surface management product and **API Sentinel**, a runtime API inventory risk mitigation product, two components of the Cequence UAP solution. This service then optimizes the discovery of your API attack surface while creating an up-to-date API inventory, resulting in a reduction in your API risk posture.

Managed Services Benefits

- **API Protection Partnership**
  Extends your team's skills with API protection expertise.
- **Global Security Insights**
  Provides key security insights gained from global attacks that ensure you have up-to-date protection for your mission critical APIs and applications.
- **Rapid Incident Response**
  Ensures every cyberattack is dealt with as quickly and effectively as possible.

Managed API Discovery and Monitoring Service at a Glance

Service Feature	Description
API Attack Surface Discovery and Runtime Inventory	Provides API Spyder and API Sentinel deployment assistance to ensure they are optimally configured to deliver continuous visibility into your API attack surface and runtime API inventory. The result is an in-depth understanding of your API risk posture and the steps required for the remediation of critical security issues.
Risk Remediation	The Cequence CQ Prime Threat Research Team researchers provide expert recommendations on key API risk areas that are discovered by API Spyder and API Sentinel. Cequence will advise your security team on how to reduce your API security risk through proper API server configurations, tighter access controls, firewall rule recommendations, application configuration and certificate management.
Reporting	Delivers periodic reports that provide insights into your attack surface and API runtime vulnerabilities. Details include API servers, exposed files, hosting providers, and a list of API risk groups prioritized by severity level (high, medium, and low) that may pose a risk to your organization.
Service Availability	Customers have phone and online access to Cequence experts for guidance on implementation.

Threat Protection

Threat Protection Managed Service leverages the CQ Prime Threat Research Team to augment your security team's expertise with threat monitoring and consulting, policy review, integration, and optimization resulting in a stronger API security posture. This managed service provides configuration and management of **Bot Defense**, the threat detection and mitigation component of the Cequence UAP solution.

Managed API Discovery and Monitoring Service at a Glance

Service Feature	Description
Proactive Threat Protection	Enables advanced monitoring of APIs to detect sophisticated cyberattacks that evade standard mitigation techniques. The CQ Prime Threat Research Team helps create an attack detection and mitigation blueprint that enables you to define, prioritize and mitigate threats more quickly.
Threat Consulting, Reporting and Policy Review	Your team is provided with a comprehensive assessment of the risks discovered at runtime that require immediate remediation. Each review includes a security policy efficacy assessment and recommendations to better mitigate targeted attacks.
Integration, Automation and Optimization	Optimizes the Bot Defense deployment to ensure rapid time-to-value and eliminate any application availability disruptions. The service provides your team with assistance in automating routine tasks and integrating into your existing security infrastructure. Customers can import third-party data to enhance analysis, or they can export the findings to their existing IT infrastructure for analysis.
World Class Threat Intelligence	The CQ Prime Threat Research Team leverages Network IQ, the largest API threat intelligence database in the world, to deliver the most up-to-date threat intelligence that is easily translated into mitigation policy to deliver real-time API protection.
Policy Customization	Working closely with your security team the CQ Prime Threat Research Team will help you fine-tune machine learning (ML) models and create use case specific security policies that detect and mitigate even the most advanced threats.
Dynamic Updates	Cequence will provide automated updates to security policies to ensure that cyberattacks are mitigated in real time to prevent the exploitation of your application.
Service Availability	Cequence provides coverage for the managed threat protection service 24/7/365, ensuring that APIs and associated applications are always monitored and protected.

API Edge Protection

Managed API Edge Protection Service augments your Bot Defense deployment with web application firewall (WAF), distributed denial of service (DDoS) protection and transport layer security (TLS) certificate provisioning. This service is only available to customers who have deployed Bot Defense and have subscribed to the Threat Protection Managed Service.

Managed API Edge Protection Service at a Glance

Service Feature	Description
WAF Configuration Services	Deploys a WAF service with a standard core rule set (CRS) that is optimized to block Open Web Application Security Project (OWASP) Top 10 attack categories.
Managed DDoS Protection	Deploys a DDoS protection service that ensures applications are protected from large scale DDoS attacks that aim to disrupt business operations.
TLS Certificate Provisioning	Provides automated provisioning and management of publicly trusted TLS certificates that enables secure communication between your application and clients.
Service Availability	Customers have phone and online access to Cequence experts for guidance on implementation.

Summary

Cequence Managed Services extends your team with additional API protection expertise to enable them to scale to meet the security challenges faced on a day-to-day basis. Partnering together, Cequence will work with your team to optimize API protection, WAF, and DDoS services to ensure you stay ahead of the ever-evolving threat landscape. The managed service enables customers to focus on security incidents in a timely, responsive, and collaborative way, making Cequence Managed Services the ideal solution for any security team, regardless of where they are in their API protection lifecycle.

CEQUENCE® SECURITY

100 S. Murphy Avenue, Suite 300, Sunnyvale, CA 94086 › 1-650-437-6338 › info@cequence.ai › www.cequence.ai