CEQUENCE

Folha de dados

Descoberta da superfície de ataque

Cequence API Spyder

À medida que as organizações evoluem, suas redes estão em constante mudança — novas aplicações são implantadas, as existentes são atualizadas e novos provedores de hospedagem são contratados por crescimento orgânico ou por fusões e aquisições. Todas essas ações impulsionam a adição de novas APIs, ampliando uma superfície de ataque já extensa. A maioria das organizações simplesmente não sabe quantas APIs possui nem onde elas estão, e esse conhecimento é fundamental para qualquer programa de segurança bem-sucedido.

Em cada organização, o API Spyder descobre uma média de:

326	197	37
Hospedeiros de API	**Domínios**	**Provedores de hospedagem**

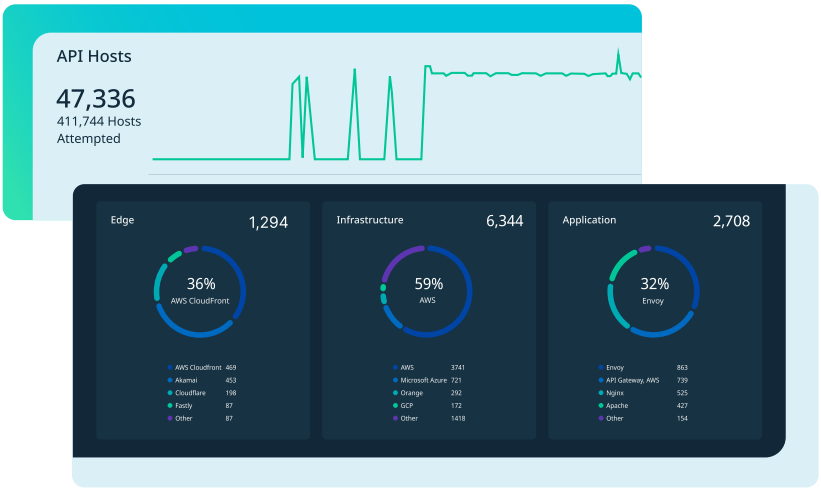
Essa superfície de ataque em constante expansão levou a novos requisitos para as equipes de segurança:

- Visibilidade completa e monitoramento de APIs voltadas para o público e provedores de hospedagem
- Identificar possíveis problemas de segurança específicos da API, como endpoints OpenAPI ou GraphQL expostos publicamente
- Relatórios personalizados sobre descobertas de superfícies de ataque externas

É fundamental ter visibilidade das APIs existentes acessíveis ao público, bem como monitorar novas APIs, especialmente aquelas que podem ter sido tornadas públicas acidentalmente, como servidores que não são de produção ou aplicativos em teste.

Visão geral do API Spyder

- **Descoberta de superfície de ataque externa,** incluindo APIs e provedores de hospedagem
- **Algoritmos configuráveis pelo usuário** para descoberta e classificação de APIs
- **Identificação de riscos de API** com percepções acionáveis
- **Relatórios centrados na pessoa** e exportação de dados detalhados



Visão geral do API Spyder

O API Spyder é uma ferramenta de descoberta baseada em SaaS que fornece a visão de um invasor sobre os recursos públicos de uma organização para encontrar hosts de API externos e identificar provedores de hospedagem não autorizados. Ele descobre metodicamente APIs e provedores de hospedagem voltados para o público, identifica problemas de segurança específicos da API e fornece relatórios de nível executivo e de fluxo de dados completo.

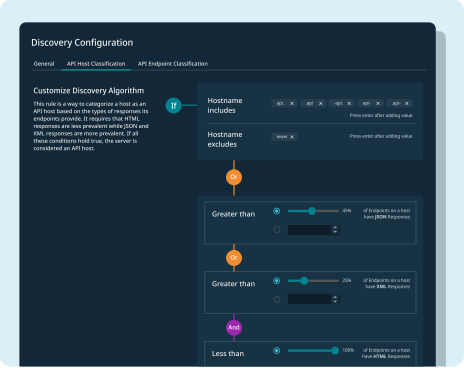
Recursos do API Spyder

Descoberta abrangente da superfície de ataque externo

Sem instalação nem agentes nos endpoints, o API Spyder executa varreduras de descoberta com base em domínios ou endereços IP para identificar hosts de API e seus provedores de hospedagem associados. Esse método permite ao API Spyder identificar hosts de API mesmo quando não estão transacionando dados, uma capacidade crítica para encontrar hosts tornados públicos por acidente, como os mal configurados ou remanescentes de testes. As varreduras podem ser feitas sob demanda ou agendadas, e também podem ser configuradas a partir de uma geografia específica, conforme necessário, por motivos de desempenho, geofencing ou privacidade de dados.

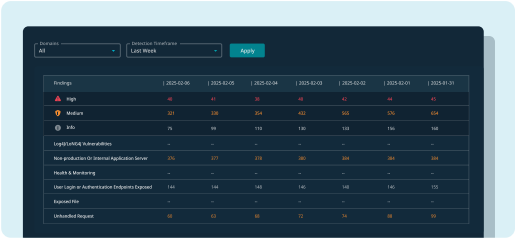
Algoritmos de descoberta e classificação de APIs configuráveis pelo usuário

Os recursos descobertos pelo API Spyder são classificados por meio de algoritmos personalizáveis pelo usuário. Cada organização e vertical é diferente, e essa capacidade permite ajustar os algoritmos de descoberta e classificação para refletir o negócio e reduzir falsos positivos. Por exemplo, é possível ajustar os algoritmos com base no número ou percentual de respostas JSON, XML ou HTML para melhorar a precisão de identificação de endpoints exclusivos ou fortemente modificados.



Identificação de riscos de API

Durante a varredura, o API Spyder descobre hosts de API com problemas conhecidos, incluindo endpoints Swagger, OpenAPI ou GraphQL expostos publicamente, ou servidores de não produção. O API Spyder categoriza essas constatações por função e severidade, com todo o contexto da requisição e da resposta. As constatações também são configuráveis pelo usuário, permitindo que as organizações priorizem os riscos que consideram mais relevantes.



Relatórios para executivos e equipes de segurança

O API Spyder fornece relatórios executivos em PDF com visualizações para uma visão de alto nível. Os dados técnicos detalhados podem ser exportados em formato Excel, incluindo todos os hosts descobertos pelo API Spyder, com detalhes de cada host de API, como endereço IP e achados de segurança.

Funciona com o Cequence AI Gateway

O Cequence AI Gateway habilita o acesso de IA baseada em agentes (agentic) a qualquer aplicação interna, externa ou SaaS, em minutos e sem necessidade de código. O API Security pode criar automaticamente especificações de API que o AI Gateway usa para criar servidores MCP, eliminando um esforço manual significativo.

O API Spyder faz parte da plataforma Cequence Unified Plataforma de proteção de APIs

A plataforma Unified API Protection da Cequence reúne descoberta, conformidade e proteção para defender as aplicações e APIs de uma organização contra ataques, abuso de lógica de negócios e fraudes. Demonstrando valor em minutos — e não em dias ou semanas —, a Cequence oferece um modelo de implantação flexível que não exige instrumentação nem modificação das aplicações. Confiada pelas maiores e mais exigentes organizações dos setores público e privado, a Cequence protege mais de 10 bilhões de interações de API por dia e 4 bilhões de contas de usuários.

CEQUENCE
5201 Great America Pkwy, Suite 240, Santa Clara, CA 95054 | 1-650-437-6338 | info@cequence.ai | www.cequence.ai