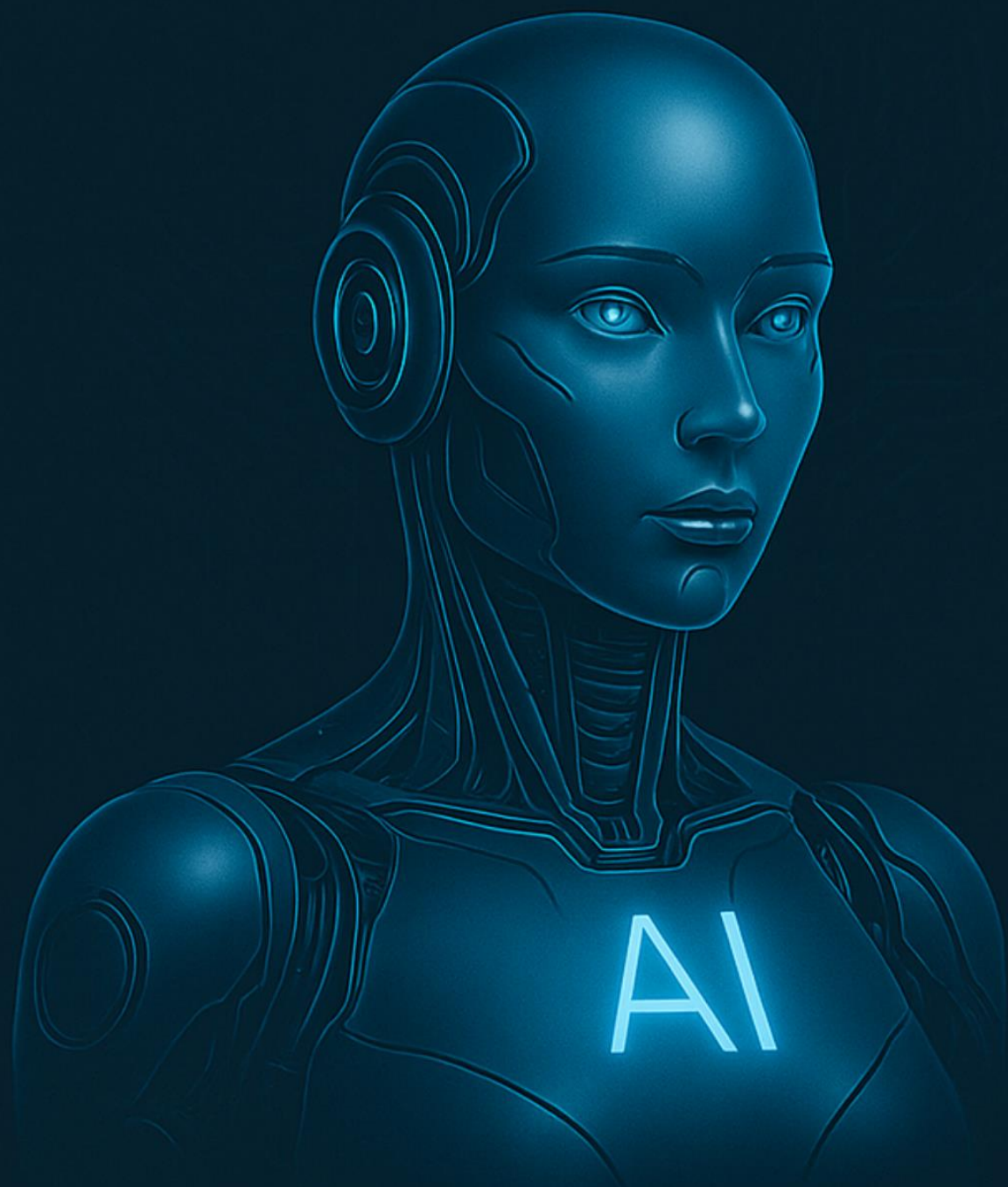




SHODAN

DO ZERO À AUTOMAÇÃO



**CVE's, Webcam, Servidores e
Simulação de Projeto para Empresas**

Sumário

GUIA COMPLETO DO SHODAN DO BÁSICO AO AVANÇADO	2
INTRODUÇÃO.....	2
COM O SHODAN, VOCÊ PODE:	3
AQUI, VAMOS EXPLORAR:.....	3
CRIANDO UMA CONTA NO SHODAN	4
1. ACESSE O SITE OFICIAL DO SHODAN	4
2. INICIANDO O CADASTRO.....	4
3. PREENCHENDO OS DADOS DE INSCRIÇÃO	5
4. CONFIRMANDO O CADASTRO	5
5. ACESSO AO PAINEL DO SHODAN	6
BENEFÍCIOS DE CRIAR UMA CONTA NO SHODAN	6
REALIZANDO PESQUISAS BÁSICAS	7
1. PESQUISA SIMPLES.....	8
2. UTILIZANDO FILTROS GEOGRÁFICOS.....	9
3. PESQUISANDO DISPOSITIVOS POR PORTA	10
REFINANDO OS RESULTADOS	11
2. PESQUISA POR VULNERABILIDADES (CVE SEARCH)	14
MONITORANDO SUA REDE	16
2. USANDO O SHODAN MONITOR PARA GERENCIAR DISPOSITIVOS EXPOSTOS	18
3. AUTOMATIZANDO O MONITORAMENTO COM A API DO SHODAN.....	20
UTILIZANDO A API DO SHODAN.....	22
1. OBTENDO SUA CHAVE DE API	23
2. CLIENTES DISPONÍVEIS E INTEGRAÇÃO COM LINGUAGENS DE PROGRAMAÇÃO.....	23
3. EXEMPLO DE USO DA API EM PYTHON.....	24
EXEMPLO DE PROJETO: IMPLEMENTANDO O SHODAN EM UMA EMPRESA	29

GUIA COMPLETO DO SHODAN

DO BÁSICO AO AVANÇADO

Neste guia, você aprenderá a **usar o Shodan de forma estratégica**, desde os conceitos básicos até as técnicas avançadas de pesquisa e automação.

Introdução

Vivemos em uma era onde a conectividade domina o mundo. A cada dia, mais dispositivos são integrados à internet, desde servidores e roteadores até câmeras de vigilância, sistemas industriais e dispositivos domésticos inteligentes. Essa interconexão facilita nossa vida de inúmeras formas, mas também abre portas para riscos que nem sempre são perceptíveis a olho nu.

O **Shodan** é uma ferramenta que joga luz sobre esse universo invisível. Ao contrário dos motores de busca convencionais, que exploram páginas da web, o Shodan é um rastreador especializado em identificar **dispositivos e serviços conectados à internet**. Com ele, é possível descobrir quais sistemas estão online, analisar configurações e até mesmo encontrar vulnerabilidades que poderiam ser exploradas.

Criado por **John Matherly** em 2009, o Shodan rapidamente ganhou notoriedade entre especialistas em segurança da informação. Para empresas, ele serve como uma poderosa ferramenta de auditoria, ajudando a mapear dispositivos expostos e a fortalecer medidas de proteção. Para pesquisadores, é um

recurso valioso na análise de tendências e ameaças cibernéticas. Seu uso, no entanto, exige **cautela e responsabilidade**, já que informações sensíveis podem ser acessadas com poucos comandos.

Com o Shodan, você pode:

- **Identificar possíveis brechas de segurança** em servidores, bancos de dados e equipamentos de rede.
- **Monitorar ativos digitais** para garantir que informações sensíveis não estejam expostas.
- **Analisar tendências e comportamentos** de ataques cibernéticos em escala global.
- **Explorar a segurança de dispositivos IoT e sistemas industriais**, verificando o nível de exposição dessas tecnologias.

Aqui, vamos explorar:

1. O funcionamento do Shodan e como ele coleta informações.
2. Como utilizar os filtros e comandos mais importantes para refinar buscas.
3. Estratégias para empresas monitorarem sua presença digital e evitarem exposições desnecessárias.
4. Maneiras de automatizar consultas e integrar o Shodan com outras ferramentas.

Ao final deste material, você estará preparado para utilizar o Shodan com confiança e precisão, ampliando suas habilidades em segurança da informação e inteligência de ameaças.

Seja bem-vindo a esta jornada!

CRIANDO UMA CONTA NO SHODAN

O Shodan permite que qualquer usuário realize buscas básicas sem precisar criar uma conta. No entanto, para desbloquear recursos avançados e aumentar a cota de pesquisas diárias, é altamente recomendável criar um perfil na plataforma.

1. Acesse o site oficial do Shodan

- Abra seu navegador preferido (Google Chrome, Mozilla Firefox, Edge ou outro).
- Digite na barra de endereços: <https://www.shodan.io>.
- Pressione Enter para acessar a página inicial do Shodan.

2. Iniciando o cadastro

- No canto superior direito da tela, clique no botão “Sign Up”.

- Você será redirecionado para a página de registro, onde precisará fornecer algumas informações básicas.

3. Preenchendo os dados de inscrição

Para criar sua conta, o Shodan solicita as seguintes informações:

- **Nome de usuário:** Escolha um nome único que será associado ao seu perfil.
- **Endereço de e-mail:** Utilize um e-mail válido, pois ele será necessário para ativar a conta e recuperar senha caso seja necessário.
- **Senha:** Crie uma senha segura, preferencialmente utilizando letras maiúsculas e minúsculas, números e caracteres especiais para aumentar a proteção.
- **Exemplo de senha segura:** Sh0dan@2024!
- **Confirmação de senha:** Digite novamente a senha para garantir que não houve erro de digitação.

4. Confirmando o cadastro

- Após preencher os campos obrigatórios, clique no botão “Sign Up” para enviar seu registro.
- O Shodan enviará um e-mail de confirmação para o endereço cadastrado.
- Acesse sua caixa de entrada e localize o e-mail com o assunto “Confirm your Shodan account”.

- Dentro do e-mail, clique no link de ativação para validar sua conta.

Observação: Se não encontrar o e-mail na caixa de entrada, verifique a pasta de spam ou lixo eletrônico.

5. Acesso ao painel do Shodan

Após confirmar sua conta, retorne ao site do Shodan e clique em “Log In” (Entrar) no canto superior direito.

- Digite o nome de usuário ou e-mail cadastrado.
- Insira sua senha e clique em “Sign In” para acessar a plataforma.

BENEFÍCIOS DE CRIAR UMA CONTA NO SHODAN

Ao se registrar, você terá acesso a recursos que não estão disponíveis para usuários anônimos, como:

- ✓ **Aumento da cota de pesquisas:** Usuários sem conta podem realizar apenas algumas consultas limitadas por dia. Com uma conta gratuita, esse limite é expandido.
- ✓ **Acesso a filtros avançados:** Contas registradas podem refinar suas buscas com maior precisão utilizando operadores avançados.

✓ **Criação de alertas personalizados:** Configure notificações para ser informado quando novos dispositivos forem encontrados com as características que você definir.

✓ **Utilização da API do Shodan:** Com uma conta, você recebe uma chave de API, que permite a automação de consultas e integração com outras ferramentas de segurança.

Caso deseje mais funcionalidades, o Shodan também oferece planos pagos que desbloqueiam pesquisas ilimitadas, downloads de dados e recursos premium.

Agora que sua conta foi criada e ativada, você está pronto para começar a explorar o Shodan e descobrir dispositivos conectados à internet!

REALIZANDO PESQUISAS BÁSICAS

Agora que você já criou sua conta no Shodan, é hora de começar a explorar os dispositivos conectados à internet. O Shodan oferece uma interface de pesquisa semelhante a um motor de busca tradicional, mas em vez de exibir páginas da web, ele retorna informações sobre servidores, roteadores, câmeras, bancos de dados e muitos outros dispositivos conectados.

Abaixo, vamos entender como realizar pesquisas básicas e como refinar os resultados para obter informações mais precisas.

1. Pesquisa Simples

A pesquisa básica no Shodan funciona de maneira similar ao Google. Basta inserir um termo na barra de pesquisa localizada na parte superior da página inicial e pressionar Enter.

Exemplos de pesquisas simples:

- **webcam** → Exibe câmeras conectadas à internet.
- **router** → Mostra roteadores públicos que podem estar expostos.
- **apache** → Retorna servidores web que utilizam o Apache.
- **raspberry** → Lista dispositivos Raspberry Pi acessíveis.
- **default password** → Pode revelar dispositivos com credenciais padrão ainda configuradas.

Interpretando os resultados

Ao realizar uma pesquisa, você verá uma lista de dispositivos correspondentes ao termo inserido. Para cada resultado, o Shodan exibe informações como:

✓ **Endereço IP** → O endereço do dispositivo encontrado.

✓ **País e cidade** → Localização aproximada do dispositivo.

✓ **Organização (ISP)** → Nome da empresa que fornece o serviço de internet.

✓ **Portas e serviços abertos** → Lista de portas acessíveis no dispositivo.

✓ **Banners de serviço** → Informações detalhadas sobre o software e versão rodando no dispositivo.

Esses detalhes são essenciais para analisar possíveis riscos de segurança e entender como um dispositivo está configurado na internet.

2. Utilizando Filtros Geográficos

Uma das funções mais úteis do Shodan é a possibilidade de restringir as pesquisas a um determinado país, região ou cidade. Para isso, usamos o filtro country:.

Exemplo de pesquisa por país:

- **webcam country:BR** → Retorna apenas câmeras expostas no Brasil.
- **router country:US** → Lista roteadores acessíveis nos Estados Unidos.
- **database country:DE** → Exibe bancos de dados disponíveis na Alemanha.

Pesquisa por cidade

Se quiser restringir ainda mais a pesquisa a uma cidade específica, use o filtro city:.

- **camera city:São Paulo** → Mostra câmeras conectadas na cidade de São Paulo.
- **mysql city:London** → Lista bancos de dados MySQL acessíveis em Londres.

Dica: Alguns dispositivos podem não ter a localização exata registrada, pois dependem da base de dados do ISP e da precisão do IP.

3. Pesquisando Dispositivos por Porta

As portas são como portões de entrada para dispositivos conectados à internet. Cada serviço online opera em portas específicas, e o Shodan permite filtrar pesquisas com base nelas.

Como funciona?

Para buscar dispositivos que possuam uma porta específica aberta, utilize o filtro port: seguido do número da porta desejada.

Exemplos de pesquisas por porta:

- **port:22** → Mostra dispositivos com SSH habilitado.
- **port:80** → Lista servidores web acessíveis via HTTP.
- **port:443** → Filtra servidores HTTPS.
- **port:3389** → Retorna computadores com Área de Trabalho Remota (RDP) exposta.

Combinação de filtros para refinar pesquisas

Você pode combinar termos de busca + filtros de porta + filtros geográficos para refinar os resultados.

✓ **apache port:80 country:US** → Retorna servidores Apache rodando na porta 80 nos Estados Unidos.

✓ **webcam port:554 city:Rio de Janeiro** → Mostra câmeras na cidade do Rio de Janeiro que utilizam a porta RTSP (usada para streaming de vídeo).

✓ **router port:23 country:RU** → Lista roteadores na Rússia com Telnet habilitado (muito perigoso para segurança).

A pesquisa básica no Shodan já permite descobrir milhares de dispositivos conectados à internet. Com apenas alguns filtros, você pode localizar servidores vulneráveis, monitorar ativos de uma região específica e encontrar serviços expostos de forma indevida.

Nos próximos passos, veremos como refinar ainda mais as buscas, explorar dispositivos vulneráveis e automatizar a coleta de dados com a API do Shodan.

REFINANDO OS RESULTADOS

Agora que já entendemos como realizar pesquisas básicas no Shodan, é hora de aprender a refinar os resultados para encontrar informações mais precisas e relevantes. Com milhões de dispositivos indexados, é essencial usar filtros avançados para reduzir o volume de dados e identificar rapidamente os dispositivos ou serviços que buscamos.

Abaixo, exploramos duas estratégias fundamentais para aprimorar suas pesquisas no Shodan: combinação de filtros e busca por vulnerabilidades conhecidas.

1. Combinação de Filtros para Pesquisas Precisas

O Shodan permite combinar múltiplos filtros para especificar exatamente o que queremos encontrar. Isso é essencial para buscas que envolvem determinados serviços, localizações ou até mesmo fabricantes específicos.

Principais filtros do Shodan

Aqui estão alguns dos filtros mais úteis que você pode usar para refinar pesquisas:

Filtro	Descrição	Exemplo
country:	Pesquisa dispositivos em um país específico.	apache country:US (Servidores Apache nos EUA)
city:	Busca dispositivos em uma cidade.	router city:São Paulo (Roteadores na cidade de São Paulo)
port:	Filtra dispositivos por portas abertas.	port:3389 (Máquinas com RDP habilitado)
org:	Pesquisa dispositivos pertencentes a uma empresa específica.	org:Microsoft (Servidores da Microsoft)

hostname:	Busca domínios específicos.	hostname:gov.br (Servidores com domínio do governo brasileiro)
os:	Pesquisa dispositivos com um sistema operacional específico.	os:Windows 10
before: / after:	Filtra por datas específicas de indexação.	before:2024-01-01 (Resultados antes de 2024)
product:	Busca por software específico rodando no dispositivo.	product:OpenSSH (Servidores rodando OpenSSH)

Exemplos de pesquisa combinando filtros

A combinação de filtros permite refinar os resultados para encontrar dispositivos com maior precisão. Veja alguns exemplos:

✓ Servidores Apache nos EUA rodando na porta 80:

apache country:US port:80

✓ Câmeras de segurança na Alemanha acessíveis via RTSP (streaming de vídeo):

camera country:DE port:554

✓ Servidores MySQL expostos na Índia:

product:mysql country:IN

✓ Sistemas SCADA (usados na indústria) expostos na Rússia:

scada country:RU

✓ Roteadores Cisco expostos no Brasil:

product:cisco country:BR

2. Pesquisa por Vulnerabilidades (CVE Search)

O Shodan também permite encontrar dispositivos vulneráveis usando identificadores de vulnerabilidades conhecidas (CVEs). Isso é extremamente útil para pesquisadores de segurança, profissionais de TI e equipes de defesa cibernética que desejam identificar sistemas desatualizados ou expostos a falhas críticas.

O que são CVEs?

CVE (Common Vulnerabilities and Exposures) é um sistema de catalogação de vulnerabilidades conhecidas, gerenciado pelo MITRE. Cada falha de segurança descoberta recebe um código único no formato:

CVE-YYYY-NÚMERO

Exemplo:

- **CVE-2021-34527** → Falha no serviço de impressão do Windows (PrintNightmare).
- **CVE-2017-0144** → Falha do SMBv1 usada pelo WannaCry.

Buscando dispositivos vulneráveis no Shodan

Para buscar dispositivos afetados por uma vulnerabilidade específica, basta usar o filtro vuln: seguido do identificador CVE.

Exemplos de pesquisas por CVE

✓ Servidores vulneráveis ao Log4Shell (CVE-2021-44228):

vuln:CVE-2021-44228

✓ Dispositivos IoT vulneráveis a falhas recentes:

iot vuln:CVE-2023-12345

Dica: O Shodan lista as vulnerabilidades conhecidas para cada dispositivo encontrado. Se um dispositivo aparecer na pesquisa, isso não significa que ele já foi explorado, mas que ele está exposto a um risco.

Agora que você aprendeu a refinar suas buscas, já pode encontrar **dispositivos específicos, serviços vulneráveis e informações estratégicas com mais precisão.**

Nos próximos passos, exploraremos como **monitorar redes empresariais, criar alertas de exposição e automatizar consultas com scripts Python.**

MONITORANDO SUA REDE

O Shodan não é apenas uma ferramenta para descobrir dispositivos conectados à internet, mas também uma plataforma de monitoramento contínuo que permite acompanhar o nível de exposição da infraestrutura digital de uma empresa, organização ou até mesmo de sua rede doméstica.

Com os recursos de alertas e o Shodan Monitor, é possível configurar notificações automáticas sempre que novos dispositivos forem detectados, quando alterações ocorrerem nos serviços expostos ou se alguma vulnerabilidade surgir. Isso é essencial para profissionais de segurança que precisam garantir que nenhum ativo crítico esteja exposto de forma indevida.

1. Configurando Alertas no Shodan

Os alertas do Shodan são uma ferramenta fundamental para acompanhar em tempo real quando dispositivos são detectados em uma determinada rede. Com eles, você pode:

- ✓ Ser notificado quando novos dispositivos aparecem na rede.
- ✓ Monitorar alterações nos serviços expostos, como portas abertas ou fechadas.

- ✓ Detectar quando uma vulnerabilidade crítica surge em um dispositivo conhecido.
- ✓ Acompanhar alterações no DNS ou mudanças em servidores da organização.

Criando um Alerta no Shodan

Para configurar um alerta e monitorar um endereço IP ou uma faixa de IPs específica, siga os passos abaixo:

1- Acesse sua conta no Shodan e vá para a seção “Alerts” clicando no link:

 <https://account.shodan.io/alerts>

2- Clique no botão “Create a new alert” para iniciar a configuração.

3- Insira um nome para o alerta, algo que ajude a identificar facilmente a sua finalidade, como:

- "Monitoramento da Infraestrutura"
- "Acompanhamento de Servidores Expandidos"

4- Informe o endereço IP ou a faixa de IPs que deseja monitorar. Você pode:

- Monitorar um único IP, por exemplo: 192.168.1.1

- Monitorar uma faixa de IPs, como: 192.168.1.0/24

5- Escolha os critérios do alerta, como:

- Mudança de portas abertas: Sempre que uma nova porta for aberta ou fechada.
- Vulnerabilidades detectadas: Caso um CVE conhecido seja associado ao IP monitorado.
- Mudança de banner: Se houver qualquer alteração nos banners de serviço de um dispositivo.

6- Defina a forma de notificação:

- O Shodan pode enviar e-mails sempre que um novo evento for registrado.
- Você pode integrar alertas com ferramentas externas, como Slack, Discord ou SIEMs.

7- Clique em “Create Alert” para finalizar a configuração.

Dica: Utilize expressões regulares e filtros avançados para personalizar seus alertas e reduzir notificações desnecessárias.

2. Usando o Shodan Monitor para Gerenciar Dispositivos Expostos

O Shodan Monitor é um painel interativo que permite visualizar e gerenciar todos os dispositivos expostos de uma organização. Com ele, é possível obter uma visão centralizada da segurança da infraestrutura digital.

O que o Shodan Monitor oferece?

Visão Geral da Exposição → Exibe um resumo dos dispositivos conectados à internet pertencentes à sua organização.

Detecção Automática de Mudanças → Acompanha serviços novos ou removidos.

Análise de Vulnerabilidades → Identifica dispositivos que possuem falhas de segurança conhecidas.

Monitoramento Contínuo → Atualiza os dados regularmente, permitindo rastrear mudanças em tempo real.

Relatórios e Exportação de Dados → Gera relatórios sobre os ativos expostos para auditoria e compliance.

Como Ativar o Shodan Monitor?

1- Acesse a página do Shodan Monitor:

👉 <https://monitor.shodan.io>

2- Clique em “Add Network” para adicionar a rede que deseja monitorar.

3- Insira o intervalo de IPs ou ASN (Autonomous System Number) da sua organização. Você pode utilizar:

- Intervalos de IPs públicos (ex: 203.0.113.0/24).

- ASN da empresa (ex: AS15169 para redes do Google).

4- O Shodan automaticamente começará a rastrear todos os dispositivos e serviços expostos dessa faixa de IPs, fornecendo uma visão detalhada da segurança da infraestrutura.

5- Visualize os dados diretamente no painel do Monitor ou exporte os relatórios em formatos como CSV e JSON para análise externa.

3. Automatizando o Monitoramento com a API do Shodan

Para empresas que desejam uma abordagem mais personalizada, o Shodan oferece uma API que permite automatizar o monitoramento da rede e integrar os dados diretamente em SOCs, SIEMs e ferramentas de resposta a incidentes.

Instalando a biblioteca do Shodan em Python

```
pip install shodan
```

Exemplo de Script para Monitoramento Automático

O código abaixo consulta o Shodan regularmente para verificar dispositivos expostos em uma faixa de IPs e notifica caso novos ativos sejam encontrados:

Se deseja monitorar dispositivos automaticamente através de scripts, instale a biblioteca do Shodan com:

```
import shodan

# Insira sua chave de API do Shodan

API_KEY = "SUA_CHAVE_API_AQUI"

# Criando uma instância do Shodan

api = shodan.Shodan(API_KEY)

# Defina a faixa de IPs que deseja monitorar

network = "203.0.113.0/24"

try:

    # Realiza a pesquisa no Shodan

    results = api.search(f"net:{network}")

    # Exibe os dispositivos encontrados

    for result in results['matches']:

        print(f"IP: {result['ip_str']}")

        print(f"Organização: {result.get('org', 'Desconhecida')}")

        print(f"Serviço: {result['port']} - {result['data'][:50]}")

        print("-" * 60)
```

```
except shodan.APIError as e:
```

```
    print(f"Erro ao consultar Shodan: {e}")
```

Esse script pode ser integrado a dashboards internos, SOCs, SIEMs ou qualquer outro sistema de monitoramento para obter notificações automáticas sobre mudanças na superfície de ataque da sua organização.

Dica: Para maior segurança, rode esse script em intervalos regulares e combine com serviços de alertas automáticos via e-mail ou webhook para ações imediatas.

- Com os alertas, é possível ser notificado em tempo real sempre que um novo dispositivo ou serviço for detectado em sua rede.
- O Shodan Monitor fornece uma visão detalhada da segurança da infraestrutura digital, permitindo que profissionais de segurança realizem auditorias e tomem decisões estratégicas.
- Utilizando a API do Shodan, é possível automatizar totalmente o processo de monitoramento e integrar as informações a sistemas internos.

UTILIZANDO A API DO SHODAN

O Shodan é uma ferramenta poderosa, mas seu verdadeiro potencial é desbloqueado quando utilizamos sua API para automatizar tarefas, integrar dados com outras plataformas e monitorar redes de forma contínua. A API do Shodan permite que você colete informações sobre dispositivos conectados à internet,

consulte vulnerabilidades, obtenha estatísticas sobre a superfície de ataque e até mesmo execute buscas programaticamente.

Se você deseja incorporar o Shodan em seus sistemas, monitorar sua rede automaticamente ou extrair grandes volumes de dados para análise, a API será sua melhor aliada.

1. Obtendo sua Chave de API

Para utilizar a API do Shodan, é necessário possuir uma chave de autenticação. Essa chave é um identificador único vinculado à sua conta e deve ser usada sempre que fizer requisições à API.

Passos para obter sua chave de API

1- Acesse sua conta no Shodan (<https://account.shodan.io/>).

2- No painel da conta, localize a seção “API Key”.

3- Sua chave de API será exibida ali. Ela terá um formato semelhante a este:

8a1b2c3d4e5f6g7h8i9j0klmnopqrstuvwxyz

Guarde essa chave com segurança! Ela é como uma senha e permite o acesso a dados do Shodan.

- Não compartilhe sua chave publicamente.
- Se precisar resetar sua chave por questões de segurança, utilize a opção “Regenerate API Key” no painel da conta.

2. Clientes Disponíveis e Integração com Linguagens de Programação

A API do Shodan pode ser acessada diretamente via requisições HTTP, mas a forma mais prática de utilizá-la é através das bibliotecas disponíveis para várias linguagens de programação.

Aqui estão algumas das linguagens suportadas oficialmente:

Language m	Biblioteca	Instalação
Python	shodan	pip install shodan
Go	github.com/ns3777k/go-shodan	go get github.com/ns3777k/go-shodan
Node.js	shodan-client	npm install shodan-client
Ruby	shodan	gem install shodan

Dica: Se a linguagem que você usa não possui uma biblioteca oficial, é possível interagir com a API via requisições REST utilizando ferramentas como cURL, Postman ou qualquer outra biblioteca HTTP disponível.

3. Exemplo de Uso da API em Python

A biblioteca oficial do Shodan para Python facilita a busca e a análise de dispositivos de forma programática.

Instalando a Biblioteca

Se ainda não tiver a biblioteca instalada, rode o seguinte comando no terminal:

```
pip install shodan
```

Fazendo uma Pesquisa Simples

Agora vamos utilizar a API do Shodan para buscar dispositivos que estejam executando servidores Apache nos EUA.

```
import shodan

# Sua chave de API

API_KEY = "SUA_CHAVE_AQUI"

# Criando uma instância do cliente Shodan

api = shodan.Shodan(API_KEY)

# Executando uma busca

try:

    resultados = api.search('apache country:US')

    print(f"Total de resultados encontrados:
    {resultados['total']}\n")

    # Exibindo os primeiros dispositivos encontrados

    for resultado in resultados['matches']:

        print(f"IP: {resultado['ip_str']}")

        print(f"Organização: {resultado.get('org',
        'Desconhecida')}")

        print(f"Serviço rodando na porta: {resultado['port']}")

        print(f"Banner: {resultado['data'][:100]}")
```

```
print("-" * 60)
```

```
except shodan.APIError as erro:
```

```
    print(f"Erro ao acessar a API: {erro}")
```

✓ Explicação do código:

- Inicializamos a biblioteca shodan e autenticamos com a chave da API.
- Realizamos uma busca por servidores Apache nos Estados Unidos.
- Iteramos sobre os resultados e extraímos IP, organização, portas abertas e banners de serviço.

Automatizando a Verificação de Vulnerabilidades

Também podemos usar a API do Shodan para encontrar dispositivos vulneráveis, utilizando identificadores CVE.

Pesquisa por Dispositivos Vulneráveis

O código abaixo encontra dispositivos vulneráveis ao CVE-2021-44228 (Log4Shell):

```
import shodan
```

```
API_KEY = "SUA_CHAVE_AQUI"
```

```
api = shodan.Shodan(API_KEY)
```

```
try:
```

```
resultados = api.search('vuln:CVE-2021-44228')

print(f"Dispositivos          vulneráveis          encontrados:
{resultados['total']}\n")

for resultado in resultados['matches']:

    print(f"IP: {resultado['ip_str']}")

    print(f"Organização:          {resultado.get('org',
'Desconhecida')}")

    print(f"Serviço: {resultado['port']}")

    print("-" * 60)

except shodan.APIError as erro:

    print(f"Erro ao acessar a API: {erro}")
```

✓ O que esse código faz?

- Busca dispositivos afetados pelo CVE-2021-44228.
- Exibe informações básicas como IP, organização e porta aberta.

Isso pode ser muito útil para analistas de segurança monitorarem sistemas internos e garantir que nenhum ativo da organização esteja vulnerável a exploits conhecidos.

Obtendo Informações Detalhadas de um IP

A API do Shodan também permite buscar informações detalhadas sobre um IP específico.

```
import shodan

API_KEY = "SUA_CHAVE_AQUI"

api = shodan.Shodan(API_KEY)

ip_alvo = "8.8.8.8" # IP do Google como exemplo

try:

    resultado = api.host(ip_alvo)

    print(f"IP: {resultado['ip_str']}")

    print(f"País: {resultado.get('country_name', 'Desconhecido')}")

    print(f"Organização: {resultado.get('org', 'N/A')}")

    print(f"AS: {resultado.get('asn', 'N/A')}")

    print(f"Portas abertas: {resultado['ports']}")

    print("-" * 60)

except shodan.APIError as erro:

    print(f"Erro ao acessar a API: {erro}")
```

✓ Explicação:

- Esse código retorna detalhes completos sobre um IP, como localização, organização, ASN e portas abertas.

- Pode ser utilizado para monitorar sua própria rede e garantir que nenhum serviço esteja exposto indevidamente.

EXEMPLO DE PROJETO: IMPLEMENTANDO O SHODAN EM UMA EMPRESA

Cenário

Uma empresa deseja mapear todos os dispositivos conectados à sua rede que estão expostos à internet, identificar possíveis vulnerabilidades e configurar alertas para novas exposições.

Etapas

1. Mapeamento de Dispositivos:

- Utilize a API do Shodan para varrer o intervalo de IPs público da empresa e listar todos os dispositivos expostos.
- Armazene as informações coletadas em um banco de dados para análise posterior.

2. Identificação de Vulnerabilidades:

- Para cada dispositivo identificado, verifique se há vulnerabilidades conhecidas associadas, utilizando o filtro vuln: da API.
- Gere relatórios detalhados destacando os dispositivos críticos e as vulnerabilidades encontradas.

3. Configuração de Alertas:

- Configure alertas no Shodan Monitor para notificar a equipe de segurança sempre que um novo dispositivo for exposto ou quando houver alterações nos dispositivos existentes.

4. Automação do Processo:

- Desenvolva scripts que executem as etapas acima em intervalos regulares, garantindo que a empresa mantenha uma visão atualizada de sua superfície de ataque.

Para aprofundar seu conhecimento e explorar todos os recursos que o Shodan oferece, visite o [Centro de Ajuda do Shodan](#), onde você encontrará guias detalhados e documentação abrangente.