PowerDMARC Threat Intel Feed API

POWERDMARC

Datasheet

PowerDMARC Threat Intel Feed API

Gain Real-Time Insight into Spoofing and Phishing Attacks

Get near real-time visibility into spoofing and phishing IP addresses using our Threat Intelligence Feed API!

Spoofing IP Detection

Retrieve data pulled from our 100k+ domain directory on IP addresses that attempted to spoof and carry out phishing attacks on domains.

Real-Time & Historical Visibility

Gain real-time and historical visibility into email threats.

Actionable Threat Intelligence

Enhance response capabilities with enriched threat intelligence.

Key Benefits

✓ Actionable Threat Intelligence

Gain real-time visibility into IP addresses engaged in spoofing attempts across your domain landscape. Instantly identify malicious sources and stay ahead of evolving threats.

✓ Automated Security Response

Seamlessly integrate the feed into your SIEM, SOAR, firewall, or Email Security Gateway (ESG) to enable automated blocking, alerting, and remediation workflows—reducing response time from hours to seconds.

✓ Stronger Security Posture

Leverage deep insights into threat actor infrastructure to fine-tune your email authentication policies (DMARC, SPF, DKIM), block risky IPs proactively, and mitigate the impact of spoofing and impersonation attacks.

Threat Intelligence Feed API Use Cases

1 Real-Time Threat Mitigation via SIEM/SOAR

Security teams and MSPs can integrate the feed with SIEM or SOAR platforms to automatically block or isolate malicious IPs in real-time, enabling faster incident response and reducing manual workload.

2 Firewall and Email Security Gateway (ESG) Enforcement

Use threat intel to update firewall or ESG rules dynamically, blocking spoofing attempts before they reach end-users—helping protect multiple client domains from a centralized platform.

3 Simplified Incident Investigation

Empower security analysts and MSPs with detailed IP attribution data to quickly trace the origin of spoofing attempts, accelerating forensics and minimizing service disruption for clients.

4 Proactive Policy Tuning for Email Authentication

Gain the insight needed to fine-tune DMARC, SPF, and DKIM records, identifying which sources are sending unauthorized emails—and which should be blocked or allowed.

5 Threat Hunting & Exposure Analysis

Feed threat data into your hunting tools to proactively search for indicators of compromise (IOCs) across your infrastructure or client networks, reducing the risk of undetected threats.

6 MSP-Centric Multitenant Monitoring

MSPs can monitor spoofing threats across multiple customer domains using a single API feed, offering premium threat protection services as a value-add to clients.

7 Executive Reporting and Risk Communication

Generate clear, data-backed reports showing which threats were blocked and which IPs were involved—helping businesses quantify risk reduction and show ROI on their security investments.

Who Is This For?

Our Threat Intelligence API is made for:

Organizations & MSPs

To protect themselves and their clients from phishing and cyber attacks

Security Analysts & Researchers

To investigate spoofing trends and understand attacker behavior.

Threat Intelligence Platforms

To enrich datasets with verified spoofing indicators.

Enterprise Security Teams

To actively defend against targeted email-based attacks.

How It Works

Using the DMARC Threat Intel Feed API is simple! Just send a request with your desired date range, and get detailed information on spoofing attempts spotted on your domains.

Response Type	Description
IP Address	The source IP that attempted to spoof your domain.
Data Source	Whether the data came from DMARC Aggregate or Forensic Reports.
Observation Count	How many times has the spoofing activity been detected from that IP.
Timestamps	The exact dates and times (in UTC) when the spoofing attempts were observed.

Threat Intel Feed API Endpoint & Usage

Endpoint:

GET /api/v1/ipinfo/spoofing-ips

Parameter	Required	Type	Description
start_date	✓	date/string	Start date of the observation period.
end_date	✗	date/string	End date of the observation period.
perPage	✗	integer	Results per page (default: 10).
page	✗	integer	Page number for pagination.

Example Request

```
GET /api/v1/ipinfo/spoofing-ips
Authorization: Bearer
YOUR_API_TOKEN
Content-Type: application/json

{
   "start_date": "2024-09-22",
   "end_date": "2024-09-23",
   "perPage": 10,
   "page": 1
}
```

Sample Response

```
{
 "data": [
   {
     "ipv4": "141.98.10.33",
     "observations": [
       {
         "date": "23-09-2024",
         "time": "N/A",
         "category": "Spoofing",
         "data_source": "DMARC Aggregate
Reports",
         "count": 111
       },
       {
         "date": "22-09-2024",
         "time": "11:01:20",
         "category": "Spoofing",
         "data_source": "DMARC Forensic
Reports",
         "count": 22
       }
     ]
   }
 ]
}
```

Getting Started with Threat Intelligence Feed API

1

Contact Sales Team

Contact us to request access to the Threat Intel Feed API.

2

Receive API Token

You'll be provided with a secure bearer token for authenticated requests.

3

Start Using the API

Begin retrieving spoofing IP data and enhance your security visibility.

Start protecting your domain from spoofing threats with real-time attack visibility!

Contact us now