XDR API Document

Contents

Credentials and Endpoint Details for accessing the API

API URL: https://xdr.zerohack.in/api/xdr-api
API Key: f5651050-3092-4b58-a9eb-208ca6d0d4dc-b61cf779-19ce-40a3-91f8-a4ed552bd41e

Getting Data from XDR Portal

To get data from XDR Portal, You can test this API via Postman Tool.
Pseudo Code for Testing the API using postman tool.

API URL: https://xdr.zerohack.in/api/xdr-api?limit=10
Method: GET
Header: {key: Enter the Application key}
Params name: value Type

Examples of the API Query for accessing the data.

- limit: numbers {10, 30,...}
- example: https://xdr.zerohack.in/api/xdr-api?limit=10

- offset: numbers {10, 30,...}
- example: https://xdr.zerohack.in/api/xdr-api?limit=10&offset=10

- order_by: String {asc, desc}
- example: https://xdr.zerohack.in/api/xdr-api?limit=10&offset=10&order_by=asc

- order_by_col_name: String {column name}
- example: https://xdr.zerohack.in/api/xdr-api?limit=10&offset=10&order_by_col_name=attack_epoch_time

- severity: number {1,2,3}(1 = High, 2 = Medium, 3 = Low)
- example: https://xdr.zerohack.in/api/xdr-api?limit=10&offset=10&order_by=asc&severity=1

- start_date: date UTC {2022-09-18 02:30:24}
- example: https://xdr.zerohack.in/api/xdr-api?limit=10&offset=10&order_by=asc&severity=1&start_date=2022-09-18 02:30:24

- end_date: date UTC {2022-09-18 02:35:30}
- example: https://xdr.zerohack.in/api/xdr-api?limit=10&offset=10&order_by=asc&start_date=2022-09-18 02:30:24&end_date=2022-09-18 02:40:25

- full example: https://xdr.zerohack.in/api/xdr-api?limit=50&offset=5&severity=2&order_by=desc&start_date=2022-09-18 02:30:24&end_date=2022-09-18 04:30:25&order_by_col_name=ml_accuracy

Sample JSON Output of the API

Sample Output:


```
{
  "message_type": "success",
  "data_len": 1,
  "data": [
    {
      "tcp_port": null,
      "ip_rep": "unknown",
      "dl_threat_class": "Detection of a Network Scan",
      "ml_severity": 1,
      "attacker_mac": "02:71:ef:c2:21:1f",
      "geoip_region_name": null,
      "target_mac_address": "02:d2:6f:17:09:db",
      "geoip_postal_code": null,
      "timezone": "UTC-0.0",
      "dl_severity": 2,
      "geoip_asn_number": null,
      "platform": "aws",
      "attack_os": "Not Available",
      "ids_threat_severity": 2.0,
      "geoip_country_name": null,
      "packet_id": 189880,
      "attacker_ip": "10.0.11.215",
      "geoip_location_properties": null,
      "udp_port": null,
      "geoip_longitude": null,
      "geoip_location_string": null,
      "service_name": "ICMP",
      "geoip_latitude": null,
      "ids_threat_type": "ET POLICY Reserved Internal IP Traffic",
      "ml_accuracy": 95,
      "attack_epoch_time": 1663471263000,
      "type_of_threat": "Lateral Movement",
      "ml_threat_class": "Attempted Administrator Privilege Gain",
```

```
        "target_os": "Linux 2.2.x-3.x",
        "@timestamp": "2022-09-18 03:24:22.973858509",
        "attack_timestamp": "2022-09-18 03:21:03",
        "target_ip": "10.0.17.150",
        "dl_accuracy": 80,
        "geoip_city": null,
        "geoip_region_code": null,
        "ids_threat_class": "Potentially Bad Traffic",
        "icmp_port": "4789.0",
        "geoip_location_array": null,
        "geoip_country_code": null,
        "geoip_asn_name": null
      }
    ]
}
```