(IO) sekoia

One view. Total control. XDR
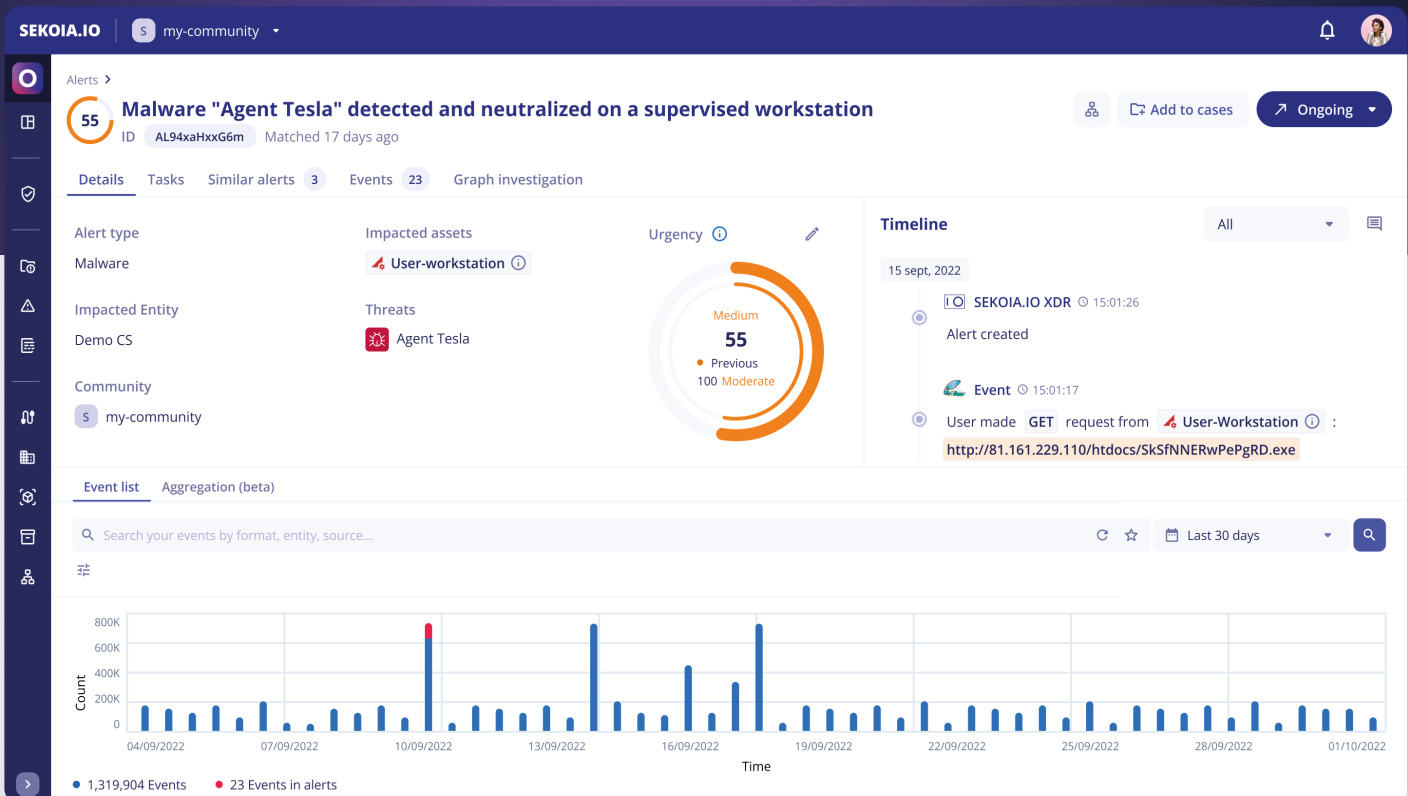
Federate

SEKOIA.IO XDR integrates easily and quickly into your security system to provide 360° coverages in only a few minutes.

Detect

Our rule catalogue combines multi-source behavior correlation, anomaly detection and proprietary cyber threat intelligence.

Respond

The management of your Information System Security is centralised from a single console. Real-time detection allows you to react immediately against any form of threat.

SEKOIA.IO   S   my-community ▾

Alerts ›

55   **Malware "Agent Tesla" detected and neutralized on a supervised workstation**   Add to cases   ↗ Ongoing ▾

ID   AL94xaHxxG6m   Matched 17 days ago

Details   Tasks   Similar alerts 3   Events 23   Graph investigation

| Alert type | Impacted assets | Urgency ✏ | Timeline | All ▾ |
| Malware | 🔺 User-workstation ⓘ | | 15 sept, 2022 |

Impacted Entity   Threats   Medium
Demo CS   ☀ Agent Tesla   **55**
                                                     Previous
Community   100 Moderate
S my-community

Timeline
● SEKOIA.IO XDR ⏱ 15:01:26
  Alert created

● Event ⏱ 15:01:17
  User made GET request from 🔺 User-Workstation ⓘ :
  http://81.161.229.110/htdocs/SkSfNNERwPePgRD.exe

Event list   Aggregation (beta)

🔍 Search your events by format, entity, source...   ↻ ☆   📅 Last 30 days ▾   🔍

Count
800K
600K
400K
200K
0
04/09/2022   07/09/2022   10/09/2022   13/09/2022   16/09/2022   19/09/2022   22/09/2022   25/09/2022   28/09/2022   01/10/2022
Time

● 1,319,904 Events   ● 23 Events in alerts

Simplify

The analyst's experience is at the heart of SEKOIA.IO. It allows users to instantly take control of the tool and increase their efficiency by a factor of 10.

Investigate

Amplify the impact of your analysts by easily manipulating terabytes of data to search, correlate, and enrich all your events and identify potential threats.

Automate

A wide range of automations frees analysts from repetitive tasks. Create your own playbooks for an even more personalised response.

Hunting threats, not false positives

Performance

Detection efficiency

- Intelligence-led real time detection
- Billions of events processed per day
- A hunt for active and undocumented threats

Our three different detection engines eliminate false positives to focus your operations on proven threats.

Rules catalog

Your Detection Effort (based on MITRE ATT&CK)

Less ▪ ■ ■ More

What do you want to cover ?

Emotet, API monitoring, Exfiltration

Threats 44   ATT&CK 194   Data sources 33

- APT39
- Turla
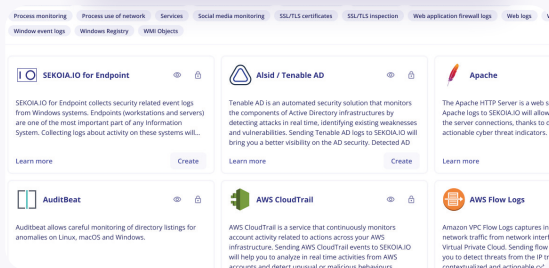- Wizard spider
- Lazarus group

Relevance of response

- MTTD < 3s (from the an event collection to the triggering of an alert)
- MTTR < 5s (from alert initiation to resolution)
- Pre-filled remediation processes

You can automate or manually perform the different actions of your responses: isolation, investigation and remediation.

Agility

Process monitoring   Process use of network   Services   Social media monitoring   SSL/TLS certificates   SSL/TLS inspection   Web application firewall logs   Web logs
Window event logs   Windows Registry   WMI Objects

SEKOIA.IO for Endpoint

SEKOIA.IO for Endpoint collects security related event logs from Windows systems. Endpoints (workstations and servers) are one of the most important part of any Information System. Collecting logs about activity on these systems will...

Learn more   Create

Alsid / Tenable AD

Tenable AD is an automated security solution that monitors the components of Active Directory infrastructures by detecting attacks in real time, identifying existing weaknesses and vulnerabilities. Sending Tenable AD to SEKOIA.IO will bring you a better visibility on the AD security. Detected AD

Learn more   Create

Apache

The Apache HTTP Server is a web se Apache HTTP Server to SEKOIA.IO will allow the server connections, thanks to da actionable cyber threat indicators.

Learn more

AuditBeat

Auditbeat allows careful monitoring of directory listings for anomalies on Linux, macOS and Windows.

AWS CloudTrail

AWS CloudTrail is a service that continuously monitors account activity related to actions across your AWS infrastructure. Sending AWS CloudTrail events to SEKOIA.IO will help you to analyze in real time activities from AWS accounts and detect unusual or malicious behaviours.

AWS Flow Logs

Amazon VPC Flow Logs captures inf network traffic from network interfa Virtual Private Cloud. Sending flow lo you to detect threats from the IP tra contextualized and actionable cyb

Integrate any tool

Our unrivalled integration capabilities allow you to connect all your equipment, regardless of its source. This means you can capitalise on your existing system and upgrade it easily.
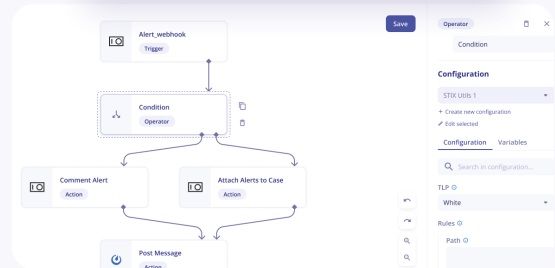
Track all your data

Control of your data is paramount, which is why the platform's interoperability facilitates your investigations, simplifies audits and avoids vendor lock-in by ensuring the portability of your data.

Deploy quickly

A Plug & Play solution that can be deployed between 12 and 72 hours, ideal for occasional supervision and for taking advantage of a particularly fast time to value.

Optimization

Alert_webhook
Trigger

Save   Operator

Condition

Configuration

STIX Utils 1

+ Create new configuration
✓ Edit selected

Condition
Operator

Configuration   Variables

Search in configuration...

Comment Alert
Action

Attach Alerts to Case
Action

TLP
White

Rules
Path

Post Message
Action

Make your analysts' work easier

A platform that adapts to users, not the other way around. The tool is entirely designed to make operations more fluid and simpler and to divide the workload by 3.

Gain bandwidth

Automation saves valuable time in the pre-qualification sorting and enriching alerts. You can then concentrate on actions where the human element is really essential.

Keep your budget under control

At SEKOIA.IO there are no surprises, the pricing only depends on one thing: the number of physical or virtual machines you want to cover.