ioThink IDS/SIEM Setup and Installation

1. About ioThink IDS/SIEM

ioThink IDS (Intrusion Detection System) and SIEM (Security Information and Event Management) can discover and track potential threats in your network. By deploying network sensors to monitor the mirrored network traffic and collecting and analyzing system logs, the threats of the entire network can be analyzed and alerted in real time:

- Who is communicating to whom?
- What files and data are currently shared?
- Is there any malicious network traffic in my network?
- Is there any data exfiltration?
- Are there new threats?
- If there are compromised machines, where are they? How to track them?

2. Hardware requirements

ioThink SIEM can be installed on any commodity hardware with minimum requirement:

- 2 Core X86-64 CPU
- 8GB RAM
- 256GB SSD Disk
- Two network interfaces (One for network mirroring)

OS:

- Linux (Centos 7 preferred)

Prerequisite:

- Docker

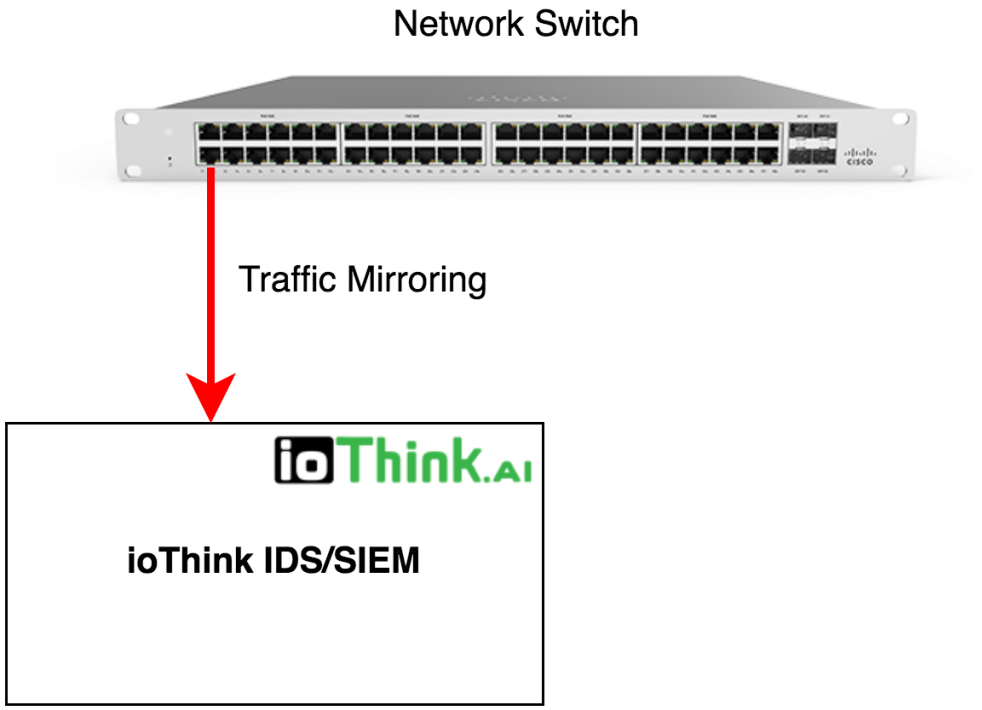
Installation time:

- ioThink SIEM can be installed within 10 minutes. Installation scripts are provided

3. Network traffic mirroring

Following diagram illustrates how to setup network traffic mirroring:

©2022 ioThink, Inc. All rights reserved



4. Software Installation

4. 1 Install Docker

You can skip the step if docker is already installed.

```
# install docker and python on centos
sudo yum install -y docker

# install docker and python on ubuntu
sudo apt-get install -y docker
```

©2022 ioThink, Inc. All rights reserved

4.2 Disable selinux

Modify /etc/selinux/config and set SELINUX to disabled

```
...
SELINUX=disabled
...
```

4.3 Download and Install

You can find the software packages at: http://software.iothink.ai/releases/

Execute the following command and enter 'yes' to continue for installation steps:

```
curl -OL http://software.iothink.ai/releases/iothink-siem_<release_version>.tgz
tar zxvf iothink-siem_<release_version>.tgz
cd iothink-siem_<release_version>
./install.sh
```

Default username and password will be displayed when the installation is complete. **Please modify the password after first login.**

Please contact us if you need any help.

5. License Key

You need a license key to be able to start the system. A temporary license key is provided with the software package. The temporary key will be valid for up to 30 days.

Please contact us if you need a permanent key. To get your permanent key please execute the following command and send us the results:

```
%/usr/local/bin/license_key_tool id
```

We will provide you the permanent license key, then you can apply the permanent key by executing :

```
%sudo /usr/local/bin/license_key_tool install <permanent_license_key>
```

©2022 ioThink, Inc. All rights reserved

6. UI

- UI address: https://<host_ip_address>:6443/siem/

7. Contact us

Website: http://www.iothink.ai
Email: info@iothink.ai
Downloads: http://software.iothink.ai/releases/

©2022 ioThink, Inc. All rights reserved