ioThink IDS/SIEM Datasheet

1. Overview

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. Features

1. Dashboard
    a. Network flow graph
    b. Quick insights of compromised hosts, suspicious hosts, hosts under attack
    c. Malware download activities
    d. Data leak activities
    e. Custom reports
2. Network Monitoring
    a. Live network traffic monitoring
    b. Sub-second query of aggregated data
    c. Signature based alerts
    d. Threat hunting
    e. Historical events search
3. App monitoring
    a. Log collection
    b. Log aggregation and search
    c. Log data reporting
4. Endpoints
    a. Asset list
    b. Machine learning powered risk reports
5. Threat Intelligence
    a. IOCs of IP, URL and file MD5

   b. Security reports generated from IOCs
6. Response Management
   a. IP blacklist
   b. Confidential file MD5
   c. Deactivate alert rules
7. Account Management
   a. Administrator
   b. User
   c. Password expiration

3. Performance Specification

ioThink Security - IDS/SIEM 2-in-1		
Specification	**Minimum Requirements**	**Recommended Requirements**
CPU Cores	2	8
Memory (RAM)	8GB	32GB
Network Interface Controllers (NICs)	2	2
Hard Drives	256GB	1TB
Performance	8k/sec	20k/sec
Detail Data Retention	14 days	30 days
Sum Data Retention	180 days	720 days

4. Contact us

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