Confidence in the Connected World

CIS Center for Internet Security®

MS-ISAC™
Multi-State Information
Sharing & Analysis Center®

For Questions:
services@cisecurity.org
www.cisecurity.org
518.880.0699

Network Security Monitoring
(Albert)

The Center for Internet Security® (CIS®), through the Multi-State Information Sharing & Analysis Center® (MS-ISAC®) offers network security monitoring services through a solution referred to as Albert. This service is available to U.S. State, Local, Tribal, and Territorial governments. Albert provides network security alerts for both traditional and advanced network threats, helping organizations identify malicious activity. This cost-effective Intrusion Detection System (IDS) uses open source software combined with the expertise of the MS-ISAC 24x7 Security Operations Center (SOC) to provide enhanced monitoring capabilities and notifications of malicious activity.

How Does Albert Work?

Albert leverages a high-performance IDS engine for the identification and reporting of malicious events. It also monitors raw network packets and converts data into a netflow format for efficient storage and analysis of historical data.

The basic lifecycle of an Albert event is as follows:

Signature fires → Alert generated & sent to 24x7 SOC → Analysis conducted in 24x7 SOC → Event notification sent

Detection & Monitoring

An IDS is only as effective as the signature set running on it. The Albert solution utilizes a unique and targeted signature set to ensure sensors rapidly recognize and alert on potentially malicious traffic occurring on the network.

MS-ISAC utilizes four main sources of signatures:

1. Commercial signatures that are optimal for detecting standard malware and crimeware
2. Advanced Persistent Threat (APT) indicators
3. Signatures developed in-house from indicators of compromise identified through forensic analysis conducted on hundreds of cyber incidents handled by the MS-ISAC Computer Emergency Response Team (CERT)
4. MS-ISAC research and open source reporting

Alerts & Reporting

No logs or data reside on the sensor. All data collected is compressed, encrypted, and sent to the MS-ISAC every few minutes for analysis. As alerts are analyzed and verified as actionable, event notifications are sent to your organization in accordance with pre-established escalation procedures. Notifications include which IP addresses are affected, the identified issues, mitigation recommendations, and an attachment containing all traffic associated with the event. Additionally, your organization may utilize the MS-ISAC API service to programmatically ingest event notifications and associated logs. Our 24x7 SOC is always available to answer questions and provide any assistance as needed.

A comprehensive monthly activity report is made available, summarizing the malicious activity identified by each sensor deployed in the organization's environment. These reports provide details for all actionable alerts for the previous month, statistics on data such as total alerts generated vs. actionable alerts, as well as a review of the total volume of monitored traffic.

What is Netflow and How is it Used?

A netflow record is a summary of a data exchange between two systems. It's based on seven distinct characteristics:

1. Source IP
2. Destination IP
3. Source port
4. Destination port
5. TCP flags
6. Number of bytes of traffic sent and received
7. Timestamp information (start, end, and duration of connection)

Traditional network security monitoring services alert on malicious activity from the time a signature is deployed, going forward. However, by leveraging netflow logs, data can be reviewed retroactively to improve the ability to search for malicious activity. This allows previous network activity to be searched for specific threats reported by partners, as well as further investigation of any major concerns identified in the network environment. Please reach out to our 24x7 SOC to request a netflow query.

Sensor Details

The Albert service utilizes commodity hardware to help provide a robust offering at a low cost. Typically, this can be run on a 1U server (or a VM for smaller installations).

We recommend supplying an Albert sensor with network traffic by way of a network tap or data aggregator (such as a gigamon) if your infrastructure already supports these options. For smaller <1Gb networks, a span port off a router or switch will work well. Please contact CIS Services for assistance with sizing your hardware.

Management

Monitoring, as well as full management of the sensor, is handled by the MS-ISAC. This includes maintaining the operating system, IDS engine, netflow tools, and signature sets.

We will work with your organization to make signature modifications upon request. We can also collaborate with you to write custom signatures to detect specific types of malicious activity on your network.

Pricing

Pricing is based on average Internet connection utilization. A one-time initiation fee per sensor applies. To find out more about network security monitoring, contact us today at **services@cisecurity.org.**

Average Internet Utilization	Monthly Fee (USD)
Up to 100Mbps	$620
>100Mbps – 1Gbps	$940
>1Gbps	$1,460