Center for Internet Security®
MS-ISAC®
EI-ISAC®

31 Tech Valley Drive
East Greenbush, NY 12061
(518) 266-3460
www.cisecurity.org

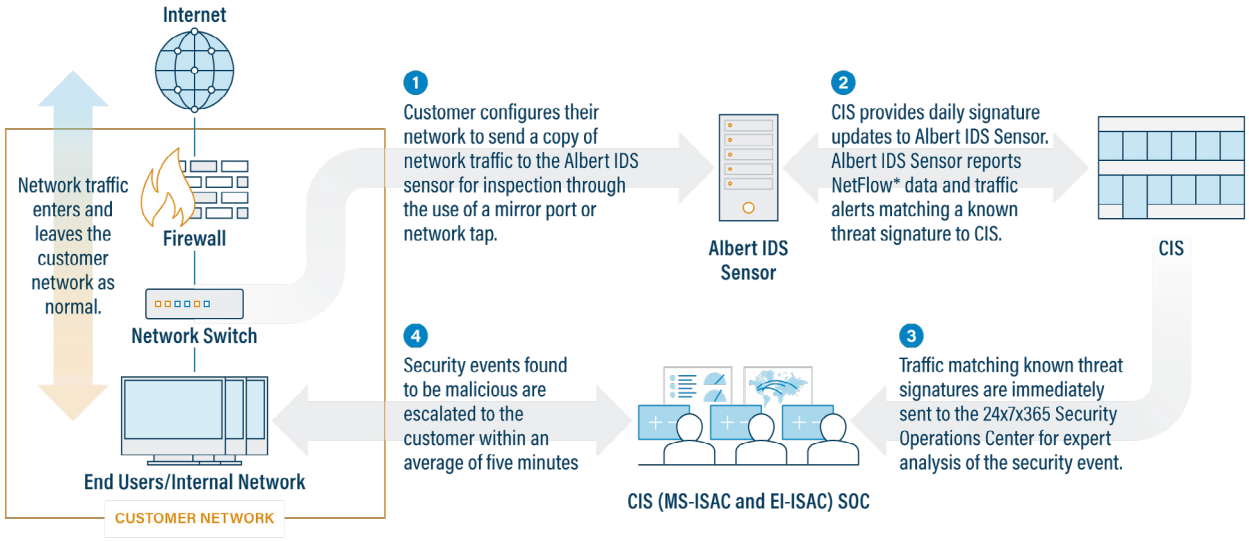
About the Albert Sensor

Albert sensors are intrusion detection systems (IDS) custom-built by the Center for Internet Security (CIS), a nonprofit nonpartisan organization, to detect cyber threats to U.S. State, Local, Tribal, and Territorial (SLTT) networks. They assist state and local governments with identifying malicious cyber activity by providing security alerts for known cyber threats.

How Albert Works

Albert sensors monitor traffic as it flows across a network to look for matches against a set of signatures for known threats. The process proceeds as follows and as illustrated in the diagram below:

1. An organization selects the network segments to be monitored and configures their network to send a copy of the selected network traffic to the Albert IDS sensor for inspection using a mirror port or network tap. This parallel configuration means that normal network traffic and speeds are unaffected by Albert.
2. CIS deploys daily threat "signatures" based on current cyber threat intelligence and reported cyber incidents to all Albert sensors to assist in identification of known malicious and anomalous activity.
3. If an Albert sensor detects a match to a known threat signature in network traffic, an alert is sent to the CIS Security Operations Center (SOC) for analysis.
4. Cybersecurity experts at the CIS SOC analyze the Albert alert and escalate to the SLTT partner if it is determined to be a credible threat. Alerts are communicated to the SLTT partner in an average of less than five minutes.



*NetFlow is a network protocol developed by Cisco for monitoring the flow and volume as well as collecting high-level metadata of IP traffic information as it passes in and out of a network interface.

Top Facts about Albert

The Albert sensor is a passive device and cannot take any active action on network traffic.

- The Albert sensor is not a firewall. It passively monitors network traffic data (including logging "NetFlow," or metadata, about network traffic). It does not block traffic and cannot negatively affect a member network or change the content or data traversing the network.

31 Tech Valley Drive
East Greenbush, NY 12061
(518) 266-3460
www.cisecurity.org

- All actions in response to an Albert alert must be taken at the SLTT partner level. The CIS SOC has no ability to "reach in" to a network and take action via an Albert sensor.
- NetFlow data is retained for six months and is used retroactively if a new threat is discovered to determine if an Albert sensor-protected network might have been impacted by the newly discovered threat.

Albert is a highly-effective, low-cost tool for detecting known threats against SLTT networks.

- Albert sensors, in combination with a layered "defense in depth" approach to cybersecurity, have proven to be highly effective in protecting against cyber threats, including known ransomware.
- While no IDS can detect 100% of malicious traffic, this powerful capability detects virtually all known threats that have documented IDS signatures.
- Albert sensors and associated SOC support are approximately one third the cost of alternative commercial products and monitoring services, and the average alert response time of under five minutes is much more rapid than alternative services.

Albert is the only intrusion detection system informed by the largest threat database specific to U.S. SLTT organizations and monitored by a Security Operations Center focused exclusively on U.S. SLTTs.

- The CIS SOC monitors alerts originating from Albert sensors 24x7x365, receiving more than 23,000 Albert alerts on average each month. They eliminate 75% of false positive alerts common to cyber defense solutions like IDS and escalate only the most credible threats, saving organizations precious time.
- The CIS SOC maintains the largest U.S. SLTT threat database informed by more than 200 threat intelligence sources. Albert sensors are updated daily with approximately 25,000 threat signatures derived from this database.

Albert is not a federal government project. It is technology produced and serviced by CIS, a trusted nonprofit serving U.S. SLTTs with cyber threat prevention, protection, response, and recovery.

- Roughly 80% of deployed Albert sensors are paid for by U.S. state and local governments. For these SLTT-funded sensors, Albert alert data and Albert NetFlow metadata is shared with Federal partners only with the explicit approval of the individual hosting state or local organization.
- The Cybersecurity and Infrastructure Security Agency (CISA) funds the deployment of the remaining Albert sensors through the Multi-State and Elections Infrastructure Information Sharing and Analysis Centers (MS- and EI-ISAC) to support cyber defense across the U.S. below the federal level. For these CISA-funded sensors, information shared with federal partners is limited to Albert alert data and Albert NetFlow metadata.

For additional information, visit https://www.cisecurity.org/services/albert-network-monitoring.