CIS Center for Internet Security®

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

Elections Infrastructure ISAC®

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

About the Albert Sensor

Albert sensors are Intrusion Detection Systems (IDS) residing on State, Local, Tribal, and Territorial (SLTT) networks. These systems provide security alerts for known cyber threats, helping state and local governments identify malicious cyber activity. The Multi State Information Sharing and Analysis Center (MS-ISAC) threat intelligence and security operations personnel curate and update daily threat "signatures" from current cyber threat intelligence and reported cyber incidents. These signatures are then deployed to all Albert sensors to assist in identification of known malicious and anomalous activity. Alerts from the Albert sensors are monitored and managed 24/7/365 by the MS-ISAC Security Operations Center (SOC). For more information, visit https://www.cisecurity.org/services/albert-network-monitoring/.

Albert sensor – Quick Facts

- The Cybersecurity and Infrastructure Security Agency (CISA) funds the development and deployment of Albert sensors through the MS-ISAC. Many Albert sensors are also self-funded by SLTT government organizations.
- Albert sensor technology was specifically designed for use in state and local government organizations.
- As of early 2022, there are over 800 Albert sensors deployed across SLTT organizations. The MS-ISAC SOC receives more than 23,000 Albert "alerts" on average, each month.
- 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.
- The Albert IDS monitors traffic data as it flows across a network to look for matches against a set of signatures for known threats. If a match is found, an alert is sent to the MS-ISAC SOC for analysis and, if warranted, escalation to the SLTT partner. Albert sensors can only see traffic to and from devices on the network where the SLTT partner has chosen to deploy them and cannot inspect the contents of any encrypted traffic.
- The MS-ISAC SOC has no ability to "reach in" to a network and take action via an Albert sensor. If an alert is generated, any response and remediation activities must be done by the SLTT partner organization.
- Albert sensors, in combination with a layered "defense in depth" approach to cybersecurity, are proven to be highly effective in protecting against cyber threats, including known ransomware. While no IDS can detect 100 percent of malicious traffic, this capability enables network defenders to detect as much malicious activity as possible, providing a more complete picture of risk faced by SLTT governments.
- A holistic approach to cybersecurity for any organization, including SLTT government organizations and election offices, means both prevention through implementation of cyber hygiene best practices and defensive capabilities through employment of additional technologies and services like Albert sensors.

The use of Albert sensors in SLTT jurisdictions across the country has helped cybersecurity professionals understand patterns of malicious activity and inform jurisdictions how to proactively protect themselves.

###