Center for Internet Security®

31 Tech Valley Drive
East Greenbush, NY 12061 USA

518.266.3460
www.cisecurity.org

The Center for Internet Security (CIS) is a nonprofit organization focused on enhancing the cyber security readiness and response of public and private sector entities. CIS operates the Multi-State Information Sharing and Analysis Center (MS-ISAC), which is designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) government entities. Through its state-of-the-art 24/7/365 cyber security operations center, CIS serves as a central resource for situational awareness and incident response for SLTT governments, and offers a number of strategic cyber security services to assist in detecting, protecting, responding to and recovering from cyber threats.

The CIS Netflow/Intrusion Detection System Monitoring and Analysis Service, known as Albert, provides our partners with a near real-time automated process that identifies and alerts on traditional and advanced threats on a network, facilitating rapid response to threats and attacks. The Albert sensor(s) provide traditional Intrusion Detection System (IDS) monitoring, along with netflow and passive DNS collection and analysis. Through its 24/7/365 Security Operations Center (SOC), CIS manages the sensor(s) to identify malicious activity, and, in accordance with escalation procedures prescribed by the partner, provides notification of malicious activity. The use of open source software allows CIS to provide enhanced monitoring capabilities in a more affordable, cost-effective way than a typical commercial IDS/IPS solution. The Albert Service is available only from CIS.

Why is the CIS Albert Service Unique?

- Government-specific focus and tailored to SLTT government's cyber security needs.
- Correlation of data from multiple public and private partners
    - Historical log analysis performed on all logs collected for specific threats reported by partners and/or trusted third parties.
    - When a major new threat is identified, CIS will search logs for prior activity. (Traditional monitoring services only alert going forward, from the date a signature is in place. There is no "look behind" to assess what activity may have already occurred.)
- Statistical analysis of traffic patterns to areas of the world known for being major cyber threats. If abnormal traffic patterns are detected, analysts review the traffic to determine the cause, looking for malicious traffic that is not detected by signatures.
- Signatures from forensic analysis of hundreds of SLTT cyber incidents are added to the signature repository.
- Integration of research on threats specific to SLTTs, including nation-state attacks.
- CIS staff permanently deployed at the National Cybersecurity and Communications Integration Center (NCCIC) in Washington, D.C, thus facilitating valuable real-time information sharing with federal partners and critical infrastructure sectors.
- Experienced cyber security analysts who review each cyber security event, which results in minimizing the number of false-positive notifications, allowing the first responder to focus on actionable events.
- Availability of an Incident Response Team for forensic and malware analysis which is of no cost to SLTT government entities.
- 24/7/365 technical, research, and remediation support for cyber security incidents.