

REN-ISAC: Information Sharing For Security Protection and Response

The Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) is an integral part of higher education's strategy to improve network security through information collection, analysis, dissemination, early warning, and response. REN-ISAC services and products are specifically designed to support the unique environment and needs of organizations connected to served higher education and research networks, and the REN-ISAC supports efforts to protect the national cyber infrastructure by participating in the formal U.S. ISAC structure. The REN-ISAC membership is comprised of security staff at member institutions: rigorous guidelines for membership and member vetting are employed to engender and maintain a community of trust requisite for sharing sensitive information regarding security incidents, vulnerabilities, and active threat. The REN-ISAC is a cooperative effort of its members, sponsoring organizations, and contributors. Current sponsoring organizations and major contributors include Indiana University, Internet2, EDUCAUSE, Louisiana State University, University of Massachusetts at Amherst, and Worcester Polytechnic University.

The REN-ISAC:

- fosters sharing of sensitive protection, incident, and response information by maintaining a trusted collaboration environment (e.g., vetted membership, secure IRC, web pages, member wiki, and webcasts);
- performs information collection, analysis, dissemination, early warning, and response assistance;
- monitors participating R&E backbone networks for DDoS events, worms, botnets, brute-force attacks, hacks, etc. (e.g., via analysis of netflow data and darknets);
- provides information products aimed at protection and response (e.g., daily status reports, alerts, notifications, lists of known sources of active threat, advisories, network monitoring views, and educational resources);
- provides security tools and information resources (e.g., Botnet Tracker which helps members to blacklist known botnet command and control hosts and to identify local bot-infected systems, a malware sandbox, and a passive DNS replication server);
- participates in various private incident mitigation communities of regional, national, and international scope, public and commercial;
- operates a 24x7 security event Watch Desk;
- participates in higher education and national efforts designed to improve protection of security of cyber infrastructures; and
- works with R&E backbone network providers for infrastructure security assurance, such as through operational security exercises involving infrastructure support, engineering, and management parties.

Benefits of Institutional Membership Include:

- participate in the information sharing trust community, with assurance for protection of sensitive information;
- access to known, trusted security contacts in the R&E community;
- receive protection and response information products including the daily Weather Report, Alerts, Advisories, and Notifications of infected and maliciously behaving systems;
- receive early warning regarding critical network threat, e.g. DDoS against local resources, new threats, and threats with changing/increasing profile;
- access to resources and tools, such as the Botnet Tracker, monitoring views, and other tools under development;
- receive protection and response information derived from REN-ISAC's participation in broad-based security protection and response communities, including relationship to DHS/US-CERT; and
- receive actionable information for cyber security protection and response.

Benefits to Network Service Providers (NSP) Include:

- proactive support for the integrity and security of services to customers;
- customers and peers are provided with protection and response for network security incidents involved or transiting the NSP network;
- the NSP receives protection and response for incidents involving its infrastructure; and;
- conformance to best-practices recommendations, such as RFC3013 *Recommended Internet Service Provider Security Services and Procedures*¹ sections 2.1–2.5.

For more information, contact:

Doug Pearson
REN-ISAC Technical Director
dodpears@ren-isac.net
+1(812)855-3846
+1(812)325-3846 cell

¹ <http://www.faqs.org/rfc/rfc3013.txt>