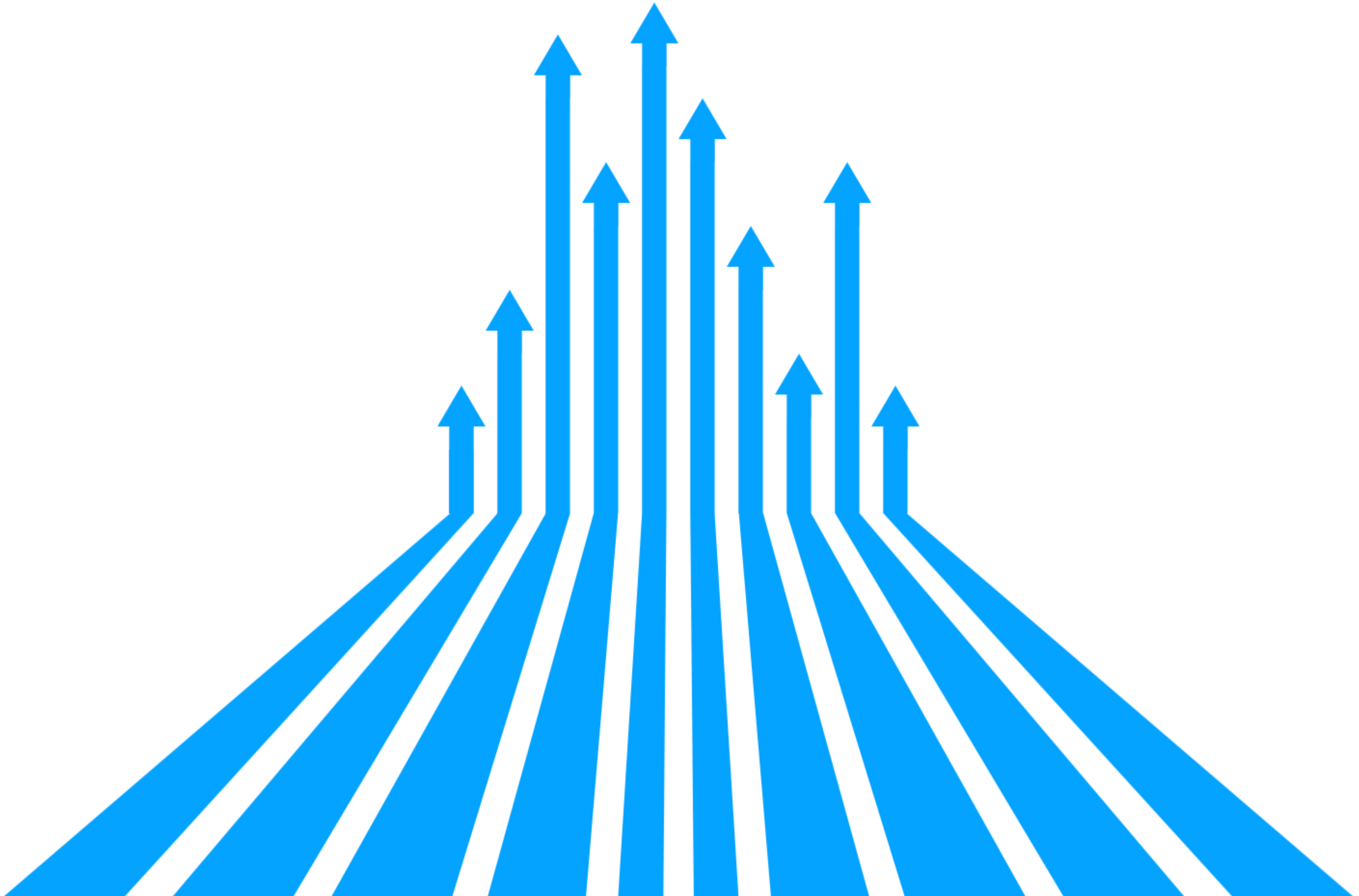
RSF

Resiliency and Security Forum



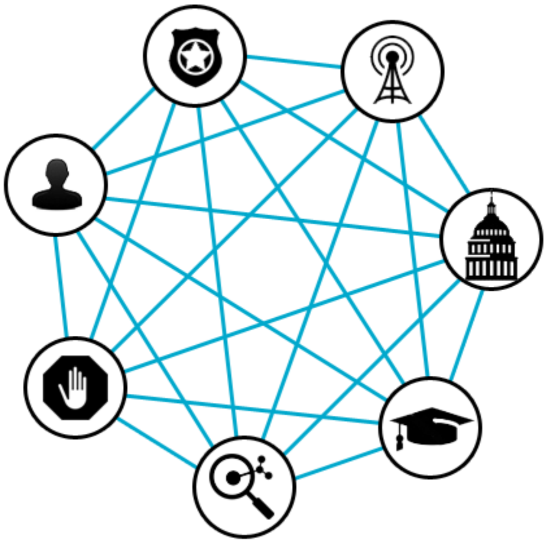
Forum Overview

The Resiliency and Security Forum (RSF) is one of ISC's special interest Forums specifically designed to support security related activities and to ensure a resilient, open and robust Internet for all. RSF projects enhance existing efforts of security professionals and organizations focused on the operational robustness, integrity and security of the Internet by proactively finding new ways to leverage their resources together to have a greater effect than they could independently. One way RSF does this is by providing infrastructure and new capabilities to the Internet security community.

Sponsorship of RSF enables ISC to develop tools, infrastructure and methods for standardized data collection, real-time processing, and efficient redistribution of results to enhance detection and mitigation of Internet crime.

Interested parties who can benefit from RSF sponsorship include:

- Network operators such as telcos, ISPs, enterprise and academic networks.
- Law enforcement organizations with international reach.
- Security companies offering anti-virus, intrusion detection, and outsourced security services.
- Research institutions including academic, public benefit, government, and commercial entities.



Interested parties can also engage with RSF via the procurement of professional services such as custom software development, consulting, or through grants/donations.

RSF Tools and Services

RSF has initiated several projects that has produced a number of tools and services that offer more transparency of suspicious activity on the Internet. These tools and services allow pro-active intervention; currently, one of our tools has the ability to actively observe and trace criminal behavior on the Internet in real-time.

All current projects and services help RSF sponsors actively participate in ensuring the operational robustness, resiliency, integrity and security of the Internet. The offered capabilities are expected to evolve with the needs of the industry.

Some of the current tools and services include:

SIE: Security Information Exchange

The Security Information Exchange (SIE) is a private framework of trusted organizations dedicated to the creation of a real-time globally trusted exchange of information. Participants can operate real time sensors that upload and/or inject live data to SIE infrastructure, and other participants can subscribe to this data either in real time through limited and anonymized download, based on public or private agreements.

The SIE infrastructure promotes trusted exchange of information among peers to tackle security issues. It provides the capability for private-public partnerships to exchange this information, and thereby fosters tighter collaboration for pro-actively detecting and reacting to malicious and criminal behavior on the Internet. All access and use, either commercial or noncommercial, must be in the public interest.

SDRN: Security Data Redistribution Network

A Security Data Redistribution Network (SDRN) is a dedicated network that redistributes security data. An SDRN expands the SIE infrastructure to allow other trusted entities to use the same tools and technologies to run their own infrastructure to exchange security related information.

There are two instances of an SDRN:

- **A Private SDRN (P-SDRN):** An SDRN that is run by a private operator that aggregates data from third parties. SIE@ISC is a P-SDRN operated by ISC.

- **An Internal SDRN (I-SDRN):** An SDRN that is operated by an entity (ISP, enterprise, government, etc.) that aggregates first party data gathered internally.

RSF recognizes the need of the industry to create islands of trust due to legal or privacy issues surrounding whom data can be shared with. If at some time in the future the legal and privacy landscapes get modified, these distinct SDRN instances have the capability to exchange information using the same tools and technologies.

NMSG: Network Message

Network Message (NMSG) is a set of tools that is used for standardizing the dissemination of real time information for effective usage. It defines both a format as well as the transport. The file format is based on Google Protocol Buffers and offers the same advantages of encoding structured data into an efficient yet extensible format. The transport is based on unidirectional UDP broadcast messages with enhanced data fragmentation and coalescing handling capabilities.

Both SIE and SDRN make extensive use of NMSG. It was developed specifically to provide a platform for efficiently passing real-time high-volume data and provides many enhancements to prior generations of work.

ISC Passive DNS

ISC has created open-source software for collecting Passive DNS replication information. The ISC collection infrastructure utilizing SIE and NMSG technology is both robust and scalable. ISC developed an enhanced Passive DNS data processing infrastructure which has evolved with the needs of researchers. ISC Passive DNS feeds into DNSDB.

DNSDB: DNS Database

The DNS Database (DNSDB) is a searchable history of DNS records that stores and indexes both the Passive DNS data, available via ISC's Security Information Exchange, as well as the authoritative DNS data that various zone operators make available. DNSDB makes it easy to search for individual DNS records as seen as different levels of the DNS tree hierarchy along with timestamps for when they were first or last seen. More importantly, DNSDB provides the ability to perform inverse look-ups based on the answers of DNS queries.

This database is frequently used as a resource for finding sources used for malicious activities. Some of its many uses include:

- Finding new domains related to existing spam or botnet campaigns.
- Enumerating IP addresses that are being used for fastflux botnets.
- Finding other DNS information utilized by known IP addresses.

Sharing DNS information broadens results from other data analysis, maps out related criminal activity, and identifies the DNS names or addresses used by cyber criminals. Access to DNSDB is only allowed for authorized and approved users.

Sponsoring RSF

To engage with RSF, interested parties choose the level of sponsorship best suited to meet their business goals from multiple benefits offered.

The table below reflects the sponsorship level and the benefits acquired:

Benefits	Supporter	Partner	Charter
Access to DNSDB	✓	✓	✓
Mailing List Membership	✓	✓	✓
Invitation to RSF Events	✓	✓	✓
Access to Technical Knowledge Base Information	✓	✓	✓
Access to Pre-Release Testing		✓	✓
Project/Feature Priority Planning		✓	✓
Discount on Engineering Support		✓	✓
Discount on RSF Products and Services		✓	✓
Discount on Consulting Services			✓
RSF Advisory Council Member			✓

The following are the details of benefits for each sponsorship category:

Access to DNSDB

Organizational access to ISC's DNSDB; providing powerful insight into the criminal activities and misuse of DNS.

Mailing List Membership

All RSF sponsors are invited to participate in open discussion of SIE and DNSDB service related issues and questions. ISC staff will participate to address questions and provide tips as well as provide support for specific issues containing confidential information. All sponsor members will have access to RSF specific information through ISC's Knowledge Base.

RSF Events

Engage in discussions, meetings and programs and receive the latest updates on upcoming RSF projects and research that will benefit the community. These events include the SIE workshops. These workshops are catalyst events – facilitating the dialog and progress amongst the SIE community. There are special closed door sessions provided at these workshops for RSF participants to share their work, analysis, and activities.

Access to Technical Knowledge Base Information

Sponsors will be able to create an account to gain access to detailed technical knowledge base information.

Access to Pre-Release Testing

Forum sponsors will be granted the capability to pre-released versions of RSF technologies for testing, and access to new technology demonstrations before wide release.

Project/Feature Priority Planning

Sponsored researchers and participants in SIE and/or RSF are given the opportunity to propose projects or capabilities that should be developed for the Internet security community and allocate resources for them. Specific features can be prioritized to serve the requirements of I-SDRN and non-ISC operated SIE nodes. Some features may require a restricted tax-deductable grant to fund the feature development.

Discount on Engineering Support

Based upon sponsorship level, special discounts are available for our sponsors for implementing capabilities that contribute and promote the resiliency of the Internet and the security industry. For more details, contact our representatives at http://rsf.isc.org/contact

Discount on Consulting Services

Special discounts are available for our sponsors that require assistance in integrating or implementing their own instances of RSF tools that benefits the resiliency of the Internet and the security industry. For more details, contact our representatives at http://rsf.isc.org/contact

Discount on RSF Products and Services

Based upon sponsorship level, RSF Forum sponsors will receive a discount on RSF supported products and services.

RSF Advisory Council

A Charter sponsor would be asked to join the RSF Advisory Council. This council will meet regularly to conduct an operations review of RSF activities, projects, and developments. The RSF Advisory Council will provide guidance on RSF activities relevant to the needs of the Internet and security industry and RSF goals.

Participating with RSF

We welcome organizations to join us in our endeavor to promote resiliency, security and maintaining a robust and open Internet.

Internet Systems Consortium is a not-for-profit organization that stands for an open and robust Internet. The Resiliency and Security Forum additionally fosters integrity, resiliency and security of the Internet. Since 1994, ISC worked with different members of the industry, many of them leaders in their markets, in carrying forward ISC's mission.

The mission of Resiliency and Security Forum is to promote and facilitate cooperation and trusted coordination among research, operational and government entities to proactively tackle security challenges on the Internet. Through the support of our sponsors and participants, ISC and RSF aim in expanding their mission across the globe and promote a progressive shift of knowledge and technology.

For more information on how your organization can join the Resiliency and Security Forum, please contact our consultants by visiting the following link http://rsf.isc.org/contact