Exploring SANS Institute Resources

The SANS Institute (Escal Institute of Advanced Technologies) is a private, non-profit organization that is globally recognized in the field of information security and specializes in training and certifications in this field. The resources on the SANS Institute website can be used by information security professionals to increase their knowledge, stay up to date and learn new things. In this report we will explore a few important SANS Institute resources.

1. **SANS Institute Training Courses:** The SANS Institute has globally recognized certification programs and offers training programs on a variety of information security topics. These programs can take the form of online or in-person trainings, certification programs or conferences.

   SANS offers a comprehensive range of training courses covering different aspects of cybersecurity, including threat intelligence, penetration testing and digital forensics. These courses are developed and delivered by industry-leading instructors and provide practical experience and skills to effectively address cyber threats. Researchers looking to deepen their expertise in specific cybersecurity areas can gain valuable knowledge and certifications by enrolling in these courses.

   Some popular courses:
   - SEC401: Security Essentials Bootcamp Style
   - SEC504: Hacker Tools, Techniques, Exploits, and Incident Handling
   - SEC560: Network Penetration Testing and Ethical Hacking
   - FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics
2. **SANS Information Security Reading Room:** is a collection of technical analysis, research, and expert opinion in the field of information security provided by the SANS Institute. These documents provide a wide range of information, with a focus on cloud security, cyber defense, cybersecurity leadership and management, industrial control systems security, incident response and threat hunting.
3. **SANS Webinars:** SANS regularly organizes webinars discussing various cybersecurity topics. These sessions include practical insights, case studies and expert advice on how to effectively identify, mitigate and respond to cyber threats. They may also include penetration testing and CTF sessions presented by experts in the field of information security, as well as demos of some products. Webinars may even be associated with some courses.
4. **SANS Survey Research:** The SANS Institute regularly conducts surveys and research to identify current trends, security threats and best practices in information security. These surveys are an important resource for assessing the current status of security professionals and organizations, learning about the challenges faced by professionals, understanding trends in the industry, and being prepared for future threats.

   Some of the surveys conducted by SANS Institute:
   1. SANS 2023 CTI Survey: Keeping Up with a Changing Threat Landscape
   2. SANS 2023 SOC Survey
   3. SANS 2022 Cyber Threat Intelligence Survey
   4. SANS 2022 SOC Survey
5. **SANS Internet Storm Center (ISC):** The ISC is a division of the SANS Institute. It was created in 2001 following the successful detection, analysis and widespread warning of the Li0n worm. The main purpose of the ISC is to continuously monitor security threats and attacks on the Internet, to understand these threats, and to provide information and guidance to the community. The ISC's website also includes many resources such as blogs that follow the latest developments

in cybersecurity, daily security diaries, analysis tools, and strategies to protect against security incidents.

Various services offered by the SANS Internet Storm Center:

1. **Journals:** Journals with commentary and analysis by SANS researchers on current security threats and incidents.
2. **Podcasts:** Podcasts featuring interviews with security experts and discussions on current security topics.
3. **Tools:**
    1. **DShield Sensor:** This sensor monitors suspicious activity and reports it to the DShield central database.
    2. **DNS Looking Glass:** A tool that allows you to query different DNS servers and see the results they return.
    3. **Honeypot (RPi/AWS):** Helps you create your own honeypots and detect malicious attacks. It can be installed on platforms such as Raspberry Pi or Amazon Web Services (AWS).
    4. **InfoSec Glossary:** lists computer and security related glossary terms and definitions.
4. **Data:**
    1. **TCP/UDP Port Activity:** Data containing TCP/UDP port activity monitored by ISC.
    2. **Port Trends:** Data that tracks trends and changes in port activity.
    3. **SSH/Telnet Scanning Activity:** Data containing SSH and Telnet scanning activities and attempts to weak usernames and passwords.
    4. **Weblogs:** The data source ISC uses to monitor honeypots and error logs of web traffic.
    5. **Threat Feeds Activity:** Contains data from various threat feeds collected by ISC.
    6. **Threat Feeds Map:** A map showing the geographical distribution of data from threat feeds.
    7. **Useful InfoSec Links:** A list of various resources that can be useful in the field of information security.
    8. **Presentations & Papers:** Presentations and articles written by ISC staff or about ISC and DShield.

REFERENCES

ISC (Internet Storm Centre) “SANS Internet Storm Centre”. Retrieved from https://isc.sans.edu/