Security operations center

A **security operations center** (**SOC**) is a centralized unit that deals with security issues on an organizational and technical level. It comprises the three building blocks people, processes, and technology for managing and enhancing an organization's security posture. Thereby, governance and compliance provide a framework, tying together these building blocks.[1] A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.[2] Typically, a SOC is equipped for access monitoring, and controlling of lighting, alarms, and vehicle barriers.[3]

Contents

IT

An information security operations center (ISOC) is a dedicated site where enterprise information systems (web sites, applications, databases, data centers and servers, networks, desktops and other endpoints) are monitored, assessed, and defended.

The United States government

The Transportation Security Administration in the United States has implemented security operations centers for most airports that have federalized security. The primary function of TSA security operations centers is to act as a communication hub for security personnel, law enforcement, airport personnel and various other agencies involved in the daily operations of airports. SOCs are manned 24-hours a day by SOC watch officers. Security operations center watch officers are trained in all aspects of airport and aviation security and are often required to work abnormal shifts. SOC watch officers also ensure that TSA personnel follow proper protocol in dealing with airport security operations. The SOC is usually the first to be notified of incidents at airports such as the discovery of prohibited items/contraband, weapons, explosives, hazardous materials as well as incidents regarding flight delays, unruly passengers, injuries, damaged equipment and various other types of potential security threats. The SOC in turn relays all information pertaining to these incidents to TSA federal security directors, law enforcement and TSA headquarters.

See also

- National SIGINT Operations Centre

References

1. Vielberth, Manfred; Böhm, Fabian; Fichtinger, Ines; Pernul, Günther (2020). "Security Operations Center: A Systematic Study and Open Challenges" (https://ieeexplore.ieee.org/document/9296846/). *IEEE Access*. **8**: 227756–227779. doi:10.1109/ACCESS.2020.3045514 (https://doi.org/10.1109%2FACCESS.2020.3045514). ISSN 2169-3536 (https://www.worldcat.org/issn/2169-3536).
2. de Leon, Sixto O. (1976). *Security: Defense Against Crime*. Manila: National Book Store. p. 17.
3. .Nadel, Barbara A. (2004). *Building Security: Handbook for Architectural Planning and Design*. McGraw-Hill. p. 2.20. ISBN 978-0-07-141171-4.
