Short Communication
Volume 10:2, 2021

Telecommunications System & Management

Open Access

Security Operations Center for OT environment – A framework

Yask *

[1]IndianOil, India

Abstract

Operational technology or OT is a category of computing and communication systems to manage, monitor and control industrial operations with a focus on the physical devices (also known as Cyber Physical Devices) and processes being used by these Cyber Physical Devices (or Systems). OT often control essential services which affect people at large, such as water and power supply, oil & gas extraction to supply, mostly all large manufacturing units etc. Additionally, operational technology is also used to monitor these critical services to prevent hazardous conditions. Manipulation of these systems and processes could have extreme impacts on the end users of these services as well as workers within operational environments.Cyberattacks on critical infrastructure and strategic industrial assets are on the rise for some years now and is now believed to be among the top five global cyber risks. The cyberattacks have cost companies millions of dollars through the disruption of services and critical operations. To keep critical systems running and protect the financial results and reputation of any organization that includes industrial processes, it's essential to improve industrial cyber security. However, securing OT environments, assessing them to determine remediation plans and strategies, and gaining visibility into them is challenging and requires different approaches than traditional IT environments.The IT environment is fairly protected and well-guarded by a Security Operations Center which keeps a constant vigil on the activities of the IT ecosystem under watch. The SOCs across the world have evolved and have reached a certain maturity in operations. However, for an OT environment, the SOC is still a new concept – primarily because the objectives of SOC of OT are different from those of IT. The mission and objectives of newer SOCs of today is about having an integrated security information and event management (SIEM) with a big data platform — complemented by workflow, automation and analytical tool. To create a SOC for OT would require re-engineering some of the OT processes, which because of being heavily dependent on the OT vendors result in a major task.Hence, there is a need to create a framework for OT SOC which helps organizations define a clear mission and objective statement for a fully operational OT SOC. The framework needs to define the roles (give directions) of the SOC team, the MSSP (if any), the OT vendors and the customer.

Biography

Yask holds a Doctorate(PhD.) in Information Technology with specialisation in OT Cyber Security. He also holds a masters degree in Cyber Law and a Bachelors in Computer Science Engineering.Currently he holds the position of CISO, IOCL and is responsible for the maintenance of Cyber-Security operations, infrastructure and governance at his organisation. He has over 2 decades of experience in steering the IT function successfully in his organisation in various capacities, with the successful execution of several IT & OT projects under his belt. His special areas of interest include - applications of OT Security, specific to O&G industry, automation models in Cyber Security and use of Machine learning to provide predictive security..

Note: This work is partly presented at event on Artificial Intelligence, IOT and Robotics (July 19-20, 2021 | Paris, France)