

Perancangan Security Operation Center (SOC): Studi kasus PT XYZ = Designing Security Operation Center (SOC): case Study PT XYZ

Kristiadi Himawan, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20468389&lokasi=lokal>

Abstrak

ABSTRAK

Peran sistem informasi dan teknologi informasi dalam sebuah organisasi sangatlah penting untuk mengatur jalannya proses bisnis menjadi lebih efektif dan efisien sehingga dapat meningkatkan kualitas layanan dan mempermudah dalam pengelolannya. Proses operasional manajemen jaringan yang sudah dilakukan di PT XYZ merupakan salah satu upaya dari perusahaan untuk menjaga performansi layanan kepada pelanggan. Penelitian ini diawali dengan adanya masalah performansi layanan yang belum mencapai target seperti yang telah ditentukan, hal ini disebabkan karena proses operasional manajemen jaringan yang sudah ada belum dapat meningkatkan performansi layanan. Salah satu faktor penting yang menjadi penyebabnya yaitu belum adanya antisipasi terhadap serangan cybersecurity yang sering muncul dan mengganggu kualitas layanan. Dari permasalahan yang ada, penelitian ini akan menjawab hal tersebut dengan pembentukan suatu Security Operation Center SOC yang akan dicapai melalui analisa arsitektur keamanan perusahaan yang akan dilihat dari perspektif bisnis. Dengan menggunakan kerangka kerja dari integrasi TOGAF dan SABSA, penelitian ini mencoba menyusun solusi yang tepat tentang bagaimana merancang SOC yang sesuai dengan kebutuhan bisnis di PT XYZ. Metode pengumpulan data yang akan dilakukan adalah melalui wawancara dengan para pemangku kepentingan, dan observasi terhadap kondisi bisnis dan kondisi infrastruktur teknologi informasi yang ada. Penelitian ini menghasilkan rancangan SOC yang dapat membantu mengatasi permasalahan keamanan cyber yang terkait dengan kualitas layanan perusahaan.

<hr>

ABSTRACT

The role of information systems and information technology in an organization is very important to manage the business process becomes more effective and efficient so it can improve the quality of service and simplify the management. The operational network management process that has been done in PT XYZ is one of the efforts of the company to maintain the service performance to the customers. This research begins with the existence of service performance problems that have not reached the target as predetermined, this is because the existing operational network management process has not been able to improve the service performance. One of the important factors that become the cause is the lack of anticipation of cybersecurity attacks that often arise and disrupt the quality of service. From that problems, this research will resolve it with the establishment of a Security Operation Center SOC which achieved through analysis of enterprise security architecture that will be viewed from a business perspective. Using framework integration TOGAF and SABSA, this research tries to devise an appropriate solution of how to design SOC that fit with the business needs of PT XYZ. Data collection methods that will be conducted are through interviews with stakeholders, and observation of business conditions and the existing information technology infrastructure. This research resulted in a SOC design that can help to address cyber security issues which related to the quality of corporate services.