Evaluasi Security Operations dan Perancangan Security Operations Center = Evaluation of Security Operations and Design of Security Operations Center: A Case Study of PT XYZ

Ari Ahmad Syarif, author

Abstrak

ABSTRAK
Rencana Strategis Teknologi Informasi PT XYZ berkomitmen menerapkan sistem pengamanan dan monitoring berupa pengembangan kehandalan keamanan infrastruktur TI. Namun kenyataannya masih ditemukan kejadian insiden keamanan yang mengakibatkan kerugian finansial maupun non-finansial, selain itu hasil pengukuran oleh Hewlet Packard Enterprise (HPE) pada tahun 2016 menyatakan tingkat kematangan security operations PT XYZ berada di level Incomplete, sehingga PT XYZ memiliki permasalahan pengelolaan security operations yang belum layak.
Penelitian ini mengevaluasi pengelolaan security operations saat ini berdasarkan hasil pengukuran HPE sebelumnya dan melakukan pengukuran tingkat kematangan secara mandiri menggunakan tools SOC-CMM. Perancangan Security Operations Center (SOC) menggunakan pendekatan Design Science Research (DSR). Metode DSR digunakan peneliti untuk menemukan solusi atas permasalahan-permasalahan aktual. Pengumpulan data dilakukan dengan studi dokumen, wawancara dan observasi. Fokus area yang diukur antara lain Business, People, Process dan Technology.
enelitian ini menghasilkan penilaian beberapa area yang perlu ditingkatkan untuk mengamankan sistem keamanan informasi. Penilaian kembali diperoleh beberapa area telah dilaksanakan sesuai rekomendasi HPE, namun masih terdapat 38 aktivitas yang belum dilaksanakan. Hasil penilaian secara mandiri menggunakan tools SOC-CMM diperoleh pencapaian tingkat kematangan di angka 1.3 (Initial) meningkat dibandingkan dengan hasil pengukuran HPE sebesar 0.78 (Incomplete). Penilaian berdasarkan framework NIST Cybersecurity diperoleh 16 area yang belum tercapai. Dibutuhkan pengembangan SIEM lebih lanjut untuk mengantisipasi secara dini ancaman. Pembangunan fasilitas SOC saat ini diperlukan, namun sebelumnya perlu dilakukan terlebih dahulu peningkatan beberapa area untuk mematangkan sistem keamanan PT XYZ.
<hr><i>ABSTRACT
nformation Technology Strategic Plan PT XYZ is committed to implementing a system of security and monitoring in the form of developing IT infrastructure security reliability. But in reality there were still security incidents that resulted in financial and non-financial losses, in addition the results of measurements by Hewlet Packard Enterprise (HPE) in 2016 stated that the maturity level of PT XYZs security operations was on incomplete level, so PT XYZ had problems managing security operations not yet feasible.
This study evaluates the current management of security operations based on previous HPE measurement results and independently measures maturity level using SOC-CMM tools. The design of the Security Operations Center (SOC) uses the Design Science Research (DSR) approach. The DSR method is used by researchers to find solutions to actual problems. Data collection is done by document study, interview and observation. The focus of the area measured includes Business, People, Process and Technology.
This research resulted in the assessment of several areas that need to be improved to secure information

security systems. Re-assessment obtained by several areas has been carried out according to HPE recommendations, but there are still 38 activities that have not been implemented. The results of the self-assessment using SOC-CMM tools obtained the achievement of the maturity level at 1.3 (Initial) increased compared to the HPE measurement result of 0.78 (Incomplete). Assessments based on the NIST Cybersecurity framework obtained 16 areas that have not been reached. Further development of SIEM is needed to anticipate threats early. The construction of the SOC facility is currently needed, but beforehand it was necessary to do an increase in several areas to finalize the security system of PT XYZ.<i/>