Evaluasi Perbandingan Metode Penentuan Prioritas Insiden Berbasis Model Respon terhadap Peringatan Intrusion Detection System pada Infrastruktur Jaringan di Sektor Strategis = Comparative Evaluation Method of Determining Priority Incident Based on Response Models to Intrusion Detection System Warnings on Network Infrastructure in the Critical Sector.

Ariani, author

Abstrak

ABSTRAK
Sistem deteksi intrusi merupakan sistem peringatan ketika ada percobaan serangan pada jaringan komputer, dengan memberikan informasi log aktivitas mencurigakan yang dapat dianalisis dan ditindaklanjuti dalam bentuk respon untuk melindungi sistem dari ancaman sebelum menyebabkan dampak lebih besar. Secara teknis, penentuan prioritas penanganan intrusi berdasarkan pada severity yang ditentukan oleh sistem atau denganskor kerentanan. Namun ada hal lain yang menjadi isu, yaitu urgensi dari sektor strategis sebagai pertahanan nasional dalam pengamanan fasilitas, jaringan, aset berbasis informasi dan fisik yang diatur oleh suatu negara dengan menetapkan sektor strategis sebagai sektor prioritas yang wajib dilindungi saat terjadi insiden sebelum berdampak lebih besar.

Pada penelitian ini, kami melakukan evaluasi beberapa metode penentuan prioritas yang diimplementasikan pada model respon yang digunakan, yaitu berdasarkan konsep manajemen waktu 4 kuadran yang telah digunakan oleh peneliti sebelumnya dengan data pengujian berupa data intrusi berbasis snort. Metode penentuan respon yang dievaluasi antara lain metode severity berdasarkan sistem deteksi intrusi berbasis snort yang disebut snort priority, rating threshold yaitu skor kerentanan, dan metode perhitungan indikator & kriteria (critical & urgent). Seiring dengan urgensi dari sektor strategis, maka pada pengujiannya metode indikator & kriteria dititik beratkan pada target yang terdaftar sebagai sektor strategis.

Penelitian ini menyimpulkan bahwa metode indikator dan kriteria sebagai faktor penentu prioritas lebih detil sehingga cukup efektif untuk diterapkan dengan model respon pada data pengujian. Selain itu, dengan metode snort priority dan rating threshold penentuan prioritas tidak memperhatikan apakah target intrusi merupakan sektor strategis atau bukan karena prioritas berdasarkan pada dampak yang telah didefinisikan oleh sistem. Namun dengan metode perhitungan indikator dan kriteria, faktor penting yang melibatkan target sektor strategis dapat didefinisikan sebagai salah satu indikator prioritas untuk menentukan kriteria critical sehingga penanganan intrusi dapat diprioritaskan lebih tinggi.
<hr>
ABSTRACT
The intrusion detection system is a warning system when there is an attempted attack on a computer network. It provides suspicious activity log information that can be analyzed and acted on in the form of a response to protect the system from threats before causing a more significant impact. Technically, determining the priority of intrusion handling is based on severity determined by the system or vulnerability

scoring. However, some issues become internal issues. A country regulates the urgency of the critical sector as a national defense in securing information-based and physical facilities, networks, and assets by establishing the critical sector as a priority sector that must be protected when an incident occurs before it has a more significant impact.

In this study, we evaluated some priority determination methods implemented in the response model used, based on the 4-quadrant time management concept used by previous researchers with test data in the form of snort-based intrusion data. The response determination methods evaluated include severity based on a snort-based intrusion detection system called snort priority, rating threshold, i.e., vulnerability score, and the purpose of calculating indicators & criteria (critical & urgent). Along with the urgency of the critical sector, the testing of indicator methods and criteria has emphasized on the targets listed as critical sectors.

This study concludes that indicator methods and criteria as determinants of priorities are more detailed so that they are effective enough to apply with response models in test data. Besides, the snort priority method and the threshold rating determination of priorities do not pay attention to whether the intrusion target is a critical sector or not because of the priority based on the impact that has been defined by the system. But with the method of calculating indicators and criteria, important factors involving critical sector targets can be identified as one of the priority indicators to determine critical criteria so that intrusion will be handling prioritized.