Evaluasi Dan Pengembangan Rules Deteksi Elasticsearch Sebagai Endpoint Detection And Response Sumber Terbuka Di Lingkungan Industrial Control System = Evaluation and Development of Detection Rules for Elasticsearch as an Open Source Endpoint Detection and Response in Industrial Control System Environments

Zegar Pradipta Putra, author

Abstrak

Peningkatan penggunaan internet di Indonesia telah menyebabkan meningkatnya ancaman siber, terutama serangan Advanced Persistent Threat (APT) yang menargetkan sistem Industrial Control System (ICS). Endpoint Detection and Response (EDR) adalah solusi keamanan yang penting untuk mendeteksi dan merespon serangan ini. Penelitian ini bertujuan untuk mengevaluasi efektivitas Elasticsearch sebagai alat EDR dalam mendeteksi serangan APT di lingkungan ICS. Fokusnya adalah pada akurasi dan efektivitas deteksi serangan menggunakan prebuilt rules Elasticsearch, serta pengembangan rules baru untuk meningkatkan kinerja deteksi. Penelitian ini menggunakan metode eksperimental dengan menerapkan Elasticsearch pada lingkungan ICS yang dibangun berdasarkan kerangka kerja GRFICS v2.0. Serangan APT disimulasikan menggunakan Caldera Adversary Emulation Platform. Evaluasi dilakukan terhadap kemampuan deteksi Elasticsearch sebelum dan sesudah penyesuaian rules. Dari 16 skenario serangan yang diuji, prebuilt rules Elasticsearch mampu mendeteksi 5 serangan, sedangkan 11 serangan lainnya memerlukan penyesuaian rules. Setelah penambahan rules baru, tingkat deteksi mencapai 100% true positive. Waktu rata-rata untuk mendeteksi serangan (MTTD) adalah 446.354 menit. Elasticsearch menunjukkan potensi yang signifikan sebagai alat EDR sumber terbuka untuk mendeteksi serangan APT di lingkungan ICS. Penelitian ini merekomendasikan pengembangan lebih lanjut pada konfigurasi Elasticsearch untuk meningkatkan akurasi dan efektivitas deteksi serangan.
.....The increasing use of the internet in Indonesia has led to a rise in cyber threats, particularly Advanced Persistent Threats (APT) targeting Industrial Control Systems (ICS). Endpoint Detection and Response (EDR) is a crucial security solution for detecting and responding to these attacks. The increasing use of the internet in Indonesia has led to a rise in cyber threats, particularly Advanced Persistent Threats (APT) targeting Industrial Control Systems (ICS). Endpoint Detection and Response (EDR) is a crucial security solution for detecting and responding to these attacks. The study uses an experimental method by implementing Elasticsearch in an ICS environment built on the GRFICS v2.0 framework. APT attacks are simulated using the Caldera Adversary Emulation Platform. Evaluation is conducted on Elasticsearch's detection capabilities before and after rule adjustments. Out of 16 attack scenarios tested, Elasticsearch's prebuilt rules detected 5 attacks, while 11 required rule adjustments. After adding new rules, the detection rate reached 100% true positive. The average time to detect an attack (MTTD) was 446,354 minutes. Elasticsearch demonstrates significant potential as an open-source EDR tool for detecting APT attacks in an ICS environment. This research recommends further development of Elasticsearch configurations to enhance the accuracy and effectiveness of attack detection.