

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian, penelitian ini berhasil membuktikan bahwa *Extended Detection and Response* (XDR) dapat meningkatkan efektivitas deteksi dan mitigasi ancaman dalam *Security Operation Center* (SOC) dan *Computer Security Incident Response Team* (CSIRT). Kesimpulan penelitian ini dibagi menjadi tiga bagian sesuai dengan tujuan penelitian, yaitu analisis dan evaluasi kinerja XDR dalam mendeteksi *malware*, identifikasi jenis serangan utama pada domain server, serta strategi peningkatan efisiensi tim SOC dan CSIRT melalui implementasi XDR.

5.1.1 Analisis dan Evaluasi Kinerja XDR dalam Deteksi *Malware* dan Respon terhadap Ancaman

Hasil penelitian menunjukkan bahwa XDR memiliki akurasi deteksi *malware* sebesar 98,3% dan mampu merespons ancaman dalam waktu kurang dari 3 detik, jauh lebih cepat dibandingkan metode tradisional yang membutuhkan 10 hingga 15 detik dalam mengkorelasikan data log dan mendeteksi serangan. Dalam skenario serangan ransomware, sistem XDR berhasil memblokir eksekusi *malware* dengan tingkat keberhasilan >98%, membuktikan bahwa XDR tidak hanya mendeteksi ancaman tetapi juga mampu melakukan mitigasi otomatis secara real-time. Selain itu, implementasi automasi berbasis AI dalam XDR berhasil mengurangi false positive hingga 40%, yang selama ini menjadi salah satu kendala dalam sistem keamanan berbasis aturan seperti SIEM. Dengan demikian, penelitian ini membuktikan bahwa XDR dapat meningkatkan kecepatan deteksi ancaman dan efektivitas mitigasi *malware* secara signifikan dalam SOC dan CSIRT.

5.1.2 Identifikasi Jenis Serangan Utama pada Domain Server dan Faktor Penyebabnya

Berdasarkan analisis terhadap insiden keamanan yang diamati selama penelitian, terdapat tiga jenis serangan utama yang sering terjadi pada domain server, yaitu *brute force attack*, *DOS attack*, dan *ransomware* atau *malware*. Serangan *brute force attack* terjadi akibat kelemahan dalam kebijakan kata sandi serta kurangnya implementasi sistem otentikasi multi-faktor (MFA). Serangan Ransomware, yang menjadi ancaman utama bagi domain server, sering kali disebabkan oleh kurangnya deteksi dini terhadap *malware* berbasis *file* dan rendahnya kesadaran pengguna terhadap phishing email. Hasil penelitian menunjukkan bahwa XDR mampu mendeteksi ketiga jenis serangan ini dengan efektivitas tinggi, terutama dalam mendeteksi pola serangan berbasis anomali yang sulit dideteksi oleh sistem keamanan tradisional. Oleh karena itu, implementasi XDR dalam SOC dan CSIRT menjadi solusi yang efektif untuk mengidentifikasi dan mengatasi serangan utama pada domain server.

5.1.3 Strategi Peningkatan Optimalisasi Tim SOC dan CSIRT melalui Implementasi XDR

Hasil penelitian ini menunjukkan bahwa implementasi XDR dapat meningkatkan optimalisasi kerja tim SOC dan CSIRT dengan mengurangi waktu analisis dan respon terhadap insiden keamanan. Dengan mengotomatiskan proses deteksi, analisis, dan mitigasi ancaman, tim SOC dapat memfokuskan sumber daya mereka pada investigasi insiden tingkat tinggi, daripada menangani false positive yang berlebihan. Selain itu, dashboard berbasis website dalam XDR memungkinkan pemantauan ancaman secara real-time, memberikan visibilitas yang lebih luas terhadap keamanan jaringan. Rekomendasi utama untuk meningkatkan efisiensi kerja tim SOC dan CSIRT meliputi penggunaan teknologi AI yang lebih canggih, seperti *Vision Transformer* (ViT) untuk deteksi ancaman zero-day, serta integrasi dengan IoT Security untuk memperluas cakupan

pemantauan ancaman. Dengan strategi ini, XDR dapat menjadi fondasi utama bagi sistem keamanan yang lebih efisien, adaptif, dan tangguh terhadap ancaman siber.

Secara keseluruhan, penelitian ini membuktikan bahwa XDR merupakan inovasi yang lebih unggul dalam mendeteksi, menganalisis, dan merespons ancaman dibandingkan metode keamanan konvensional. Dengan integrasi kecerdasan buatan (AI), korelasi data *multi-layer*, serta respons otomatis, sistem ini dapat mempercepat deteksi ancaman, mengurangi false positive, serta meningkatkan efektivitas pengawasan real-time dalam SOC dan CSIRT.

Rekomendasi pengembangan yang diusulkan dalam penelitian ini, adalah penggunaan Vision Transformer (ViT) untuk meningkatkan deteksi serangan zero-day, integrasi dengan teknologi IoT Security, serta pengujian dalam skenario jaringan yang lebih kompleks, menjadi arah penting untuk memastikan bahwa XDR terus berkembang sebagai solusi keamanan siber yang lebih tangguh dan adaptif.

5.2 Saran

Berdasarkan hasil penelitian, berikut beberapa saran yang dapat dipertimbangkan untuk pengembangan lebih lanjut:

1. Optimalisasi Algoritma K-Means

Perlu dilakukan pengujian dengan parameter yang lebih variatif dalam algoritma K-Means untuk meningkatkan akurasi dalam mengelompokkan data log SIEM.

2. Integrasi dengan *Machine Learning* Lanjutan

Untuk meningkatkan akurasi deteksi, sistem dapat dikembangkan lebih lanjut dengan mengintegrasikan metode *machine learning* lain seperti *Random Forest* atau *Deep Learning*.

3. Peningkatan Sistem Notifikasi dan Automasi

Implementasi sistem notifikasi *real-time* yang lebih responsif dapat membantu administrator dalam menangani ancaman lebih cepat dan efisien.

4. Evaluasi False Positives dan False Negatives

Perlu dilakukan analisis lebih lanjut terhadap *false positives* dan *false negatives* yang terjadi dalam sistem agar deteksi ancaman menjadi lebih akurat dan tidak mengganggu operasional normal sistem.

5. Pengembangan Infrastruktur untuk Skalabilitas

Untuk memastikan sistem dapat menangani jumlah data log yang besar, perlu dilakukan peningkatan infrastruktur, baik dalam aspek komputasi maupun penyimpanan data.

Dengan adanya pengembangan lebih lanjut berdasarkan saran di atas, diharapkan sistem ini dapat semakin optimal dalam meningkatkan keamanan siber pada lingkungan yang lebih luas.