JIMATEK: JURNAL ILMIAH MAHASISWA TEKNIK

JIMATEK is Available Online at:
https://ojs-teknik.usni.ac.id/index.php/JIMAT
Vol. 03 No. 1 (2025), pages: 47-51
DOI: www.doi.org/10.59134/jimat.v3i1.761

ANALISA KEAMANAN WEBSITE MENGGUNAKAN *AQUA SECURITY*: INTEGRASI BIG DATA DALAM DETEKSI DAN MITIGASI ANCAMAN PADA LINGKUNGAN KONTAINER

Sukarno Bahat Nauli
Universitas Satya Negara Indonesia
sukarnobahat@usni.ac.id
Hernalom Sitorus
Universitas Satya Negara Indonesia
hernalom@usni.ac.id
Melani Indah Sari Manik
Universitas Satya Negara Indonesia
melani.indah@usni.ac.id
Sultan Sabdo Pandito
Universitas Satya Negara Indonesia
sultansabdo@gmail.com

Keywords
Container security; Aqua Security; Docker; Kubernetes; Big Data; Threat detection

ABSTRACT
This study evaluates the effectiveness of Aqua Security for threat detection and mitigation in containerized environments running a web application and a Big Data module. The testbed uses Docker and Kubernetes. Methods include image scanning, runtime policies, RBAC, and compliance checks, complemented by attack simulations and log analysis. Results show that Aqua identifies vulnerabilities and anomalous runtime activities and provides policy recommendations that accelerate response and reduce risk in a laboratory setting. Limitations include constrained scale and workload diversity. In conclusion, integrating Aqua Security is effective as a detection-and-mitigation layer for a web + Big Data container architecture and is recommended for further evaluation at production scale.

Kata kunci
Keamanan kontainer; Aqua Security; Docker; Kubernetes; Big Data; Deteksi ancaman

ABSTRAK
Penelitian ini mengevaluasi efektivitas Aqua Security untuk deteksi dan mitigasi ancaman pada lingkungan kontainer yang menjalankan aplikasi web dan modul Big Data. Arsitektur uji menggunakan Docker dan Kubernetes. Metode meliputi pemindaian image, kebijakan runtime, RBAC, dan pemeriksaan kepatuhan, disertai simulasi serangan serta analisis log. Hasil menunjukkan Aqua mampu mengidentifikasi kerentanan dan aktivitas anomali saat runtime serta memberi rekomendasi kebijakan yang mempercepat respons dan menurunkan risiko pada skenario laboratorium. Keterbatasan penelitian terletak pada skala uji dan variasi beban yang terbatas. Kesimpulannya, integrasi Aqua Security efektif sebagai lapisan deteksi dan mitigasi pada arsitektur kontainer web + Big Data, dan direkomendasikan untuk diuji lanjut pada skala produksi.

PENDAHULUAN

Perkembangan teknologi digital dan komputasi awan mendorong penggunaan kontainer seperti Docker dan Kubernetes karena kemampuannya membuat sistem lebih fleksibel, skalabel, dan portabel. Meski demikian, kontainerisasi menghadirkan tantangan keamanan baru seperti image yang rentan, akses tidak sah, privilege

escalation, hingga serangan injeksi, yang sulit diatasi dengan metode tradisional (Yuliandari et al., 2010).

Untuk menjawab masalah tersebut, hadir Aqua Security sebagai platform keamanan cloud-native yang mendukung image scanning, runtime protection, serta otomasi kebijakan keamanan dari tahap build hingga run. Beberapa penelitian menyoroti pentingnya integrasi keamanan dalam siklus hidup kontainer (Handayanto et al., 2018), namun kajian yang mengombinasikan Aqua Security dengan analisis Big Data masih jarang dilakukan.

Penelitian ini mengembangkan sistem berbasis web dan Big Data yang dikontainerisasi dengan Docker, dijalankan di Kubernetes, serta diamankan dengan Aqua Security. Kebaruan penelitian terletak pada pemanfaatan analisis Big Data secara real-time untuk mengevaluasi kemampuan Aqua Security dalam mendeteksi dan memitigasi ancaman pada sistem kontainer.

METODOLOGI PENELITIAN

- **Pendekatan:** Eksperimen simulatif (uji keamanan Aqua Security pada Docker & Kubernetes dengan analisis Big Data).
- **Objek Penelitian:** Aqua Security, Docker, Kubernetes, Website dummy, Big Data (CSV).
- **Waktu & Tempat:** April–Juli 2025, laboratorium virtual berbasis Ubuntu 22.04 LTS.
- **Tahapan Penelitian:**
  - Instalasi OS (April 2025)
  - Setup Aqua Security (Mei 2025)
  - Simulasi serangan & pengumpulan data (Mei–Juni 2025)
  - Analisis & evaluasi (Juni–Juli 2025)
  - Penyusunan laporan (Juli 2025)
- **Metode Pengumpulan Data:**
  - Wawancara (praktisi/ahli)
  - Observasi (respon Aqua Security & logging)
  - Studi pustaka (literatur & dokumentasi resmi)
- **Perancangan Sistem:**
  - Pembuatan Dockerfile & build image
  - Deployment dengan Kubernetes (YAML)
  - Integrasi Aqua Security (scanning & runtime)
  - Simulasi serangan (injection, brute force, privilege escalation, unauthorized access, container exec)
  - Logging & analisis data
- **Analisis Data:**
  - Klasifikasi log
  - Pemetaan serangan
  - Perbandingan sebelum–sesudah
  - Visualisasi pola anomali
- **Evaluasi Sistem:**
  - Tingkat deteksi ancaman
  - Waktu respons
  - Efektivitas mitigasi
  - False positive/false negative
  - Dampak pada performa website
- **Kebutuhan Penelitian:**
  - Hardware: Laptop/PC i5/Ryzen 5, RAM 8–16 GB, SSD 256 GB
  - Software: Docker, Kubernetes, Aqua Security, Ubuntu, PHP, MySQL, VS Code, Python/Spreadsheet

HASIL DAN PEMBAHASAN

- **Arsitektur Sistem**
  - Website dummy menampilkan data transaksi dari CSV (*Big Data*) + MySQL.
  - Sistem Big Data (CSV Viewer) membaca ribuan entri CSV.
  - Lingkungan: Docker (isolasi), Kubernetes (orkestrasi), Aqua Security (scanning & runtime protection).
  - Host: Ubuntu 22.04 LTS.
- **Perancangan & Pengembangan**
  - VS Code digunakan untuk penulisan kode, Dockerfile, dan YAML deployment.
  - Dua deployment utama: *deployment-bigdata* dan *deployment-sultan* (Website + DB).
  - Image dibangun → dipush ke Docker Hub → dijalankan di Kubernetes.
- **Implementasi di Kubernetes**
  - Semua pod, service, dan volume berjalan stabil (9 deployments, 17 pods, 1 daemon set).
  - Monitoring dilakukan melalui Kubernetes Dashboard & Aqua Security Dashboard.

  Integrasi Aqua Security
  - Aqua Enforcer terhubung (Connected) dan aktif memantau runtime.
  - Hasil scanning menunjukkan risiko **Critical** pada image (*website-sultan, bigdata, myadmin, mysql*).
  - Deteksi kerentanan: >60 CVE dengan kategori Critical, High, Medium.
- **Respon terhadap Simulasi Serangan**
  - **Brute Force Login (Hydra)** → berhasil terdeteksi (High severity), dicatat di log, serangan digagalkan.
  - **Container Exec** → upaya akses langsung ke container diblokir otomatis.
  - Runtime policies (Block Reverse Shell, Fork Guard, Port Scanning Detection) aktif memblokir aktivitas berbahaya.
- **Analisis Statistik Aqua Security**
  - 77,8% container berisiko Critical.
  - 21 image diuji, semua memiliki kerentanan (Low–Critical).
  - Tidak ada malware/sensitive data terdeteksi.
  - Runtime event dominan: *block-root-privilege* & *reverse shell test* (deteksi 99–100%).
- **Audit & Logging**
  - Total 144 event log tercatat (Success, Detect, Block).
  - Audit menunjukkan *docker exec* & brute force berhasil diblokir sesuai konfigurasi.
- **Strategi Mitigasi**
  1. *Hardening* & update image (hapus paket tidak perlu, rebuild library).
  2. Integrasi scanner di pipeline CI/CD.
  3. Isolasi jaringan & prinsip *least privilege*.
  4. Pemantauan real-time dengan Aqua Enforcer.
  5. Segmentasi host scanner & cluster scanner.
  6. Aktivasi runtime policies (*Block Exec, Reverse Shell, Fork Guard*).
- **Evaluasi Efektivitas**
  - Docker: semua image (website, bigdata, MySQL, phpMyAdmin) berjalan stabil dengan port mapping.
  - Kubernetes: deployment konsisten, workload berjalan normal.
  - Aqua Security: berhasil mendeteksi & memblokir serangan utama (brute force & container exec).
  - Visualisasi: ditemukan 7 kerentanan exploitable tingkat tinggi (glibc, curl, Go library).

KESIMPULAN

Penelitian ini berhasil merancang dan mengimplementasikan sistem keamanan berbasis **Docker, Kubernetes, dan Aqua Security** untuk melindungi

aplikasi web dan sistem *Big Data*. Hasil pengujian menunjukkan bahwa Aqua Security efektif dalam:

1. Melakukan pemindaian kerentanan (*image scanning*) pada setiap container.
2. Memberikan proteksi saat runtime terhadap serangan berisiko tinggi seperti *Brute Force Login* dan *Container Exec*.
3. Menghasilkan log insiden yang akurat untuk mendukung analisis dan mitigasi lanjutan.

Dengan penerapan *Runtime Policy* yang tepat, sistem mampu mendeteksi, memblokir, sekaligus meminimalkan dampak ancaman pada lingkungan kontainerisasi.

Prospek pengembangan penelitian ini dapat diarahkan pada:

- Integrasi dengan pipeline **CI/CD** untuk otomatisasi pemindaian sebelum deployment.
- Pemanfaatan teknik **machine learning** dalam analisis log untuk meningkatkan akurasi deteksi ancaman.
- Implementasi pada lingkungan produksi berskala besar untuk mengukur efektivitas sistem dalam kondisi nyata.

DAFTAR PUSTAKA

Adhikari, S., & Baidya, S. (2024). Cyber security in containerization platforms: A comparative study of security challenges, measures and best practices. *arXiv preprint*. https://doi.org/10.48550/arXiv.2404.18082

Aqua Security Docs. (2025). *Aqua Platform Documentation*. https://docs.aquasec.com

Burns, B., Grant, B., Oppenheimer, D., Brewer, E., & Wilkes, J. (2016). Borg, Omega, and Kubernetes. *Communications of the ACM, 59*(5), 50–57. https://doi.org/10.1145/2890784

Chekole, E. G., Zhou, J., & Ochoa, M. (2023). On the security of containers: Threat modeling, attack analysis, and mitigation strategies. *Computers & Security, 131*, 103299. https://doi.org/10.1016/j.cose.2023.103299

Combe, T., Martin, A., & Di Pietro, R. (2016). To Docker or not to Docker: A security perspective. *IEEE Cloud Computing, 3*(5), 54–62. https://doi.org/10.1109/MCC.2016.91

Docker Documentation. (2025). *Get started with Docker*. https://docs.docker.com/get-started/

Kubernetes Documentation. (2025). *Production-grade container orchestration*. https://kubernetes.io/docs/home/

Merkel, D. (2014). Docker: Lightweight Linux containers for consistent development and deployment. *Linux Journal, 2014*(239), 2. https://dl.acm.org/doi/10.5555/2600239.2600241

Morić, Z., Dakić, V., & Čavala, T. (2025). Security hardening and compliance assessment of Kubernetes control plane and workloads. *Journal of Cybersecurity and Privacy, 5*(2), 30. https://doi.org/10.3390/jcp5020030

Novitawaty, N., & Hendradi, P. (2022). Penggunaan perangkat lunak robot untuk otomatisasi dan mempercepat proses integrasi sistem dan manusia dalam berbagai proses bisnis. *Prosiding, 2*, 255–273. https://doi.org/10.59134/prosidng.v2i-.133

Sharma, K. (2025). A deep dive into container security challenges, strategies, and resource isolation in orchestrated environments. *Advances in Intelligent Systems Research (RAISD 2025)*. https://doi.org/10.2991/978-94-6463-787-8_38

Sutabri, T., Rian, H., Hendradi, P., & Febrianto, F. (2020, January). Designing the

autogate pass dashboard application with Android-based responsive web design technology. In *Proceedings of the First International Conference of Science, Engineering and Technology*.

Wong, A. Y., Chekole, E. G., & Zhou, J. (2021). Threat modeling and security analysis of containers: A survey. *arXiv preprint*. https://doi.org/10.48550/arXiv.2111.11475