**LAPORAN KEGIATAN**

**SECURING YOUR SOFTWARE DEVELOPMENT PIPELINE - CYBER SECURITY PERSPECTIVE**



**Disusun Oleh :**

**NAMA DOSEN : Ahmad Jurnaidi Wahidin**

**NIDN : 0315059301**

**FAKULTAS TEKNIK DAN INFORMATIKA**

**PROGRAM STUDI TEKNOLOGI INFORMASI**

**UNIVERSITAS BINA SARANA INFORMATIKA**

**TAHUN 2024**

**==========================================================**

**LAPORAN HASIL KEGIATAN**

**Securing Your Software Development Pipeline - Cyber Security Perspective**

**==========================================================**

**BAB I**

**PENDAHULUAN**

1. **Latar Belakang Kegiatan**

Dalam dunia teknologi informasi yang berkembang pesat, ancaman siber telah menjadi salah satu tantangan terbesar bagi organisasi dan individu yang terlibat dalam pengembangan perangkat lunak. Pipeline pengembangan perangkat lunak, yang mencakup seluruh tahapan mulai dari perencanaan, pengkodean, pengujian, hingga penerapan, merupakan tulang punggung dari setiap proyek perangkat lunak modern. Namun, setiap tahapan dalam pipeline ini menghadirkan potensi risiko yang dapat dimanfaatkan oleh pelaku kejahatan siber.

Kemajuan dalam metodologi pengembangan perangkat lunak, seperti Continuous Integration (CI) dan Continuous Deployment (CD), meskipun menawarkan efisiensi yang signifikan, juga membuka pintu bagi ancaman baru yang membutuhkan perhatian serius. Oleh karena itu, menjaga keamanan pipeline pengembangan perangkat lunak bukan lagi sekadar pilihan, melainkan kebutuhan yang mendesak.

Webinar ini diadakan dengan tujuan untuk memberikan pengetahuan dan pemahaman mendalam mengenai bagaimana menjaga keamanan dalam pipeline pengembangan perangkat lunak dari perspektif keamanan siber. Dengan menghadirkan seorang ahli di bidang ini, diharapkan peserta dapat memperoleh wawasan yang lebih luas tentang praktik-praktik terbaik dalam melindungi pipeline pengembangan mereka dari ancaman siber..

1. **Maksud dan Tujuan Kegiatan**

Kegiatan ini dirancang dengan beberapa tujuan utama, di antaranya:

1. Meningkatkan Kesadaran dan Pemahaman

Memberikan pengetahuan mendalam mengenai ancaman siber yang dapat mengintai setiap tahap dalam pipeline pengembangan perangkat lunak. Peserta diharapkan dapat memahami risiko-risiko ini dan bagaimana cara mitigasinya.

1. Menambah Wawasan Praktis

Menyediakan wawasan yang konkret mengenai metode, alat, dan teknik yang dapat digunakan untuk mengamankan pipeline pengembangan perangkat lunak. Hal ini meliputi implementasi langkah-langkah keamanan yang dapat diintegrasikan ke dalam proses CI/CD.

1. Memfasilitasi Diskusi Profesional

Membuka ruang untuk diskusi yang produktif antara peserta dari berbagai latar belakang, termasuk mahasiswa, akademisi, dan praktisi industri. Diskusi ini diharapkan dapat menghasilkan pemikiran-pemikiran baru tentang bagaimana meningkatkan keamanan dalam pengembangan perangkat lunak.

**BAB II**

**LAPORAN KEGIATAN**

1. **Bentuk Kegiatan**

Webinar ini dilaksanakan dalam bentuk seminar online via Zoom Meeting dengan menghadirkan pemateri yang ahli di bidangnya. Pemateri yang diundang untuk mengisi sesi ini adalah Yanto Setiawan, S.Kom, MTI, CEH, CIPMP, seorang dosen di BINUS Online Learning sekaligus Kepala IT di Koperasi Astra International. Beliau memiliki pengalaman luas di bidang keamanan siber dan pengembangan perangkat lunak, yang membuatnya sangat kompeten dalam membahas topik ini.

1. **Pelaksanaan Kegiatan**

Kegiatan webinar dilaksanakan pada :

Tanggal : 10 Agustus 2024

Waktu : 10:00 – 12:00

Tempat : *Zoom Video Conference*

Join Zoom Meeting : <https://us06web.zoom.us/j/93316724492?pwd=Mxdbbcrp4sZQX33akOOZx9bUdZcpB0.1>

Meeting ID: 933 1672 4492

Passcode: 019283

**2.3. Hasil Kegiatan**



Webinar ini dihadiri oleh sekitar 450 peserta yang terdiri dari mahasiswa, dosen, dan profesional industri. Kehadiran yang tinggi mencerminkan tingginya minat terhadap topik keamanan dalam pipeline pengembangan perangkat lunak. Sepanjang sesi, peserta tampak sangat antusias dan terlibat aktif dalam diskusi.

Pemateri memulai sesi dengan penjelasan mengenai konsep dasar CI/CD dan mengapa keamanan menjadi elemen yang sangat penting dalam pipeline ini. Beliau menekankan bahwa setiap langkah dalam pipeline pengembangan, mulai dari integrasi kode hingga penerapan, memiliki potensi risiko keamanan yang harus dikelola dengan baik. Pemateri juga membahas pentingnya melakukan penilaian risiko secara berkala untuk mengidentifikasi dan mengatasi kerentanan yang mungkin muncul.

Berikut ini adalah beberapa poin utama yang dibahas selama webinar:

1. Manfaat Keamanan dalam CI/CD

Pemateri menekankan bahwa keamanan tidak boleh dianggap sebagai tambahan di akhir proses, tetapi harus diintegrasikan sejak awal dalam pipeline. Hal ini mencakup penggunaan alat deteksi kerentanan yang secara otomatis dapat mengidentifikasi dan melaporkan potensi masalah keamanan.

1. Alat dan Teknik Keamanan

Webinar ini juga membahas berbagai alat dan teknik yang dapat digunakan untuk mengamankan pipeline. Beberapa di antaranya termasuk pengaturan kontrol akses yang ketat, penggunaan enkripsi end-to-end, serta penerapan otentikasi multi-faktor untuk akses ke sistem CI/CD.

1. Studi Kasus

Sebagai bagian dari sesi, pemateri menyajikan beberapa studi kasus tentang bagaimana perusahaan teknologi terkemuka, seperti Tesla dan Amazon, telah mengimplementasikan keamanan siber yang kuat dalam pipeline pengembangan mereka. Contoh-contoh ini menunjukkan bagaimana perusahaan tersebut berhasil meningkatkan efisiensi operasional mereka sambil meminimalkan risiko keamanan.

Selain itu, sesi tanya jawab yang interaktif memberikan kesempatan kepada peserta untuk mengeksplorasi lebih dalam topik yang telah dibahas. Pertanyaan yang diajukan oleh peserta mencerminkan keingintahuan yang tinggi dan menunjukkan bahwa topik ini sangat relevan dengan tantangan yang mereka hadapi dalam pekerjaan sehari-hari.

**BAB III**

**PENUTUP**

1. **Kesimpulan**

Secara keseluruhan, webinar ini berhasil memberikan pemahaman yang lebih mendalam mengenai pentingnya keamanan siber dalam pipeline pengembangan perangkat lunak. Materi yang disampaikan memberikan wawasan baru yang dapat langsung diterapkan oleh peserta dalam proyek mereka. Peserta tidak hanya mendapatkan pengetahuan teoritis, tetapi juga panduan praktis tentang bagaimana mengamankan pipeline pengembangan mereka dari ancaman siber.

1. **Saran**

Sebagai tindak lanjut dari webinar ini, disarankan agar kegiatan serupa terus dilakukan secara berkala dengan fokus yang lebih mendalam pada aspek praktis penerapan keamanan siber dalam pipeline pengembangan perangkat lunak. Selain itu, kolaborasi antara akademisi dan praktisi industri perlu ditingkatkan untuk memperkuat pemahaman dan keterampilan peserta dalam menghadapi ancaman siber yang semakin kompleks. Pendampingan khusus bagi mahasiswa yang tertarik untuk mengembangkan proyek berbasis keamanan siber juga akan sangat bermanfaat, guna mendorong inovasi dan kesiapan mereka dalam memasuki dunia kerja yang menuntut kemampuan teknis yang tinggi. Dengan pendekatan ini, diharapkan sumber daya manusia yang dihasilkan dapat lebih tangguh dan siap berkontribusi dalam menciptakan lingkungan pengembangan perangkat lunak yang aman dan efisien.