# "TRAINING CYBER SECURITY ANALYST SERTIFIKASI BNSP"

## I. DESCRIPTION:

Pada transformasi digital, ancaman cyber berkembang semakin kompleks dan terstruktur. Oleh karena itu, organisasi pemerintah maupun swasta wajib memperkuat sistem keamanan informasi mereka. Selain itu, data kini menjadi aset strategis yang harus dilindungi secara maksimal. Jika terjadi insiden keamanan, maka kerugian finansial, reputasi, bahkan hilangnya kepercayaan publik dapat terjadi. Analis keamanan siber memainkan peran kunci dalam melindungi infrastruktur TI dan data dari serangan cyber, kebocoran informasi, dan kerusakan reputasi. Keterampilan dalam mengidentifikasi kerentanan, menganalisis risiko, dan merespons insiden keamanan siber menjadi sangat kritis.

Training Cyber Security Analyst ditujukan untuk memperkuat keterampilan dan pengetahuan peserta dalam menghadapi ancaman siber serta meningkatkan kemampuan mereka dalam melindungi aset dan informasi. Kemudian Sertifikasi Cyber Security Analyst BNSP menjadi sangat penting. Melalui sertifikasi resmi dari Badan Nasional Sertifikasi Profesi (BNSP), profesional keamanan siber dapat membuktikan kompetensinya sesuai standar nasional. Dengan demikian, Anda tidak hanya memiliki kemampuan teknis, tetapi juga pengakuan resmi yang meningkatkan kredibilitas profesional.

Pelatihan yang membahas mengenai Cyber Security Analyst BNSP memerlukan waktu tersendiri dan bimbingan yang profesional. Untuk itu kami bekerjasama dengan Lembaga Sertifikasi Profesi (LSP) Informatika dengan Surat Keputusan Nomor: KEP.2375/BNSP/XI/2023 dan Lisensi Nomor: BNSP-LSP-317-ID dengan asessor yang berpengalaman. Kami berkeyakinan training ini akan memberikan nilai lebih untuk karyawan/ staff yang mengikuti pelatihan ini.

## II. BENEFIT & ADVANTAGE:

Melalui kegiatan pembelajaran ini diharapkan peserta:

- Mengembangkan keterampilan dalam merespons dan memitigasi insiden keamanan siber.
- Memahami ancaman siber terkini dan metodologi serangan.
- Menguasai teknik dan alat analisis keamanan siber.
- Memperkuat pengetahuan tentang kebijakan dan regulasi keamanan siber. Mengembangkan keahlian dan pengetahuan mendalam tentang konsep dan teknologi keamanan informasi.
- Membantu melindungi organisasi dari ancaman keamanan yang terus berkembang.
- Menanggapi kebutuhan meningkatnya keamanan data pribadi baik di tingkat pribadi maupun perusahaan.

- Menjalankan tanggung jawab etis terhadap data pengguna dan informasi sensitif.
- Membekali individu dengan keterampilan untuk mengidentifikasi, mencegah, dan merespons terhadap ancaman cyber.
- Memastikan pemahaman dan kepatuhan terhadap standar keamanan cyber yang berlaku di industri tertentu.
- Berkontribusi pada inovasi teknologi dengan memastikan produk dan layanan tetap aman.
- Membantu menjaga privasi individu dan melindungi data pribadi dari penyalahgunaan.

## III. COURSE TOPICS :

| | | |
|---|---|---|
| 1. | J.62090.001.01 | Menerapkan Prinsip Perlindungan Informasi |
| 2. | J.620900.026.02 | Melakukan Instalasi Software Aplikasi |
| 3. | J.62090.003.01 | Menerapkan Prinsip Keamanan Informasi untuk Penggunaan Jaringan Internet |
| 4. | J.62090.004.01 | Menerapkan Prinsip Keamanan Informasi pada Transaksi Elektronik |
| 5. | J.62090.005.01 | Menyusun Dokumen Kebijakan Keamanan Informasi |
| 6. | J.62090.006.01 | Melaksanakan Kebijakan Keamanan Informasi |
| 7. | J.62090.012.01 | Mengaplikasikan Ketentuan/Persyaratan Keamanan Informasi |
| 8. | J.62090.020.01 | Mengelola Log |
| 9. | J.62090.024.01 | Melaksanakan Pencatatan Asset |
| 10. | J.62090.032.01 | Menerapkan Kontrol Akses Berdasarkan Konsep/Metodologi yang Telah Ditetapkan |
| 11. | J.62090.033.01 | Mengidentifikasi Serangan-Serangan Terhadap Kontrol Akses |

A. Dasar-dasar Keamanan Cyber
   - Pengenalan keamanan cyber dan pentingnya
   - Ancaman, kerentanan, dan risiko dalam keamanan cyber
   - Prinsip-prinsip dan praktik terbaik dalam keamanan cyber

B. Teknik Analisis Keamanan
   - Pemantauan dan deteksi ancaman cyber
   - Analisis kerentanan dan penilaian risiko
   - Penggunaan alat dan software dalam analisis keamanan

C. Manajemen Insiden dan Respon
   - Protokol dan prosedur respons insiden
   - Forensik digital dan investigasi
   - Kesiapan dan pemulihan dari insiden keamanan cyber

D. Kebijakan dan Regulasi Keamanan Cyber
   - Kebijakan keamanan dan standar industri
   - Regulasi dan kepatuhan hukum
   - Kesadaran dan pelatihan keamanan cyber

E. Studi Kasus dan Simulasi

- Latihan simulasi insiden keamanan
- Analisis kasus nyata serangan cyber
- Diskusi strategi dan solusi keamanan

F. Persiapan Ujian Sertifikasi BNSP
   - Review unit kompetensi BNSP
   - Simulasi ujian sertifikasi
   - Tanya jawab dan diskusi studi kasus

## IV. SYARAT PESERTA :

Berkas-berkas yang dipersiapkan:

1. Copy KTP.
2. Curriculum Vitae (CV)/ Daftar Riwayat Hidup terkini.
3. Copy Ijasah terakhir.
4. Pas foto 3×4 sebanyak 2 lembar berlatar belakang warna merah dan berpakaian rapi (tidak diperbolehkan menggunakan kaos).
5. Masing-masing peserta wajib membawa laptop