1

TENTANG KAMI

SUROSOWAN CYBER

Visi dan Misi

Meningkatkan minat dan pengetahuan peserta didik di bidang teknologi informasi dan komunikasi untuk mencetak generasi IT berkualitas yang berdampak positif bagi daerah.

Program Unggulan Komunitas (GRATIS)

1. Akademi
2. Seminar
3. Roadshow
4. Sharing Session

Rifki Nugraha
Ketua Komunitas

Bramantyo Ardi
Wakil Ketua Komunitas

2

DOKUMENTASI KEGIATAN

SUROSOWAN CYBER

00

3

MEMBONGKAR RAHASIA DIBALIK SERANGAN SIBER

4

01

INTERMEZZO KASUS KEAMANAN SIBER

5

MEMAHAMI KEAMANAN SIBER

02

Keamanan siber praktik melindungi sistem, jaringan, dan data dari serangan digital yang dapat merugikan individu maupun organisasi.

01

Definisi: Keamanan siber mencakup perlindungan aset digital dari akses tidak sah, kerusakan, atau pencurian data.

02

Ancaman & Risiko: Malware, phishing, ransomware, dan pelanggaran data mengancam sistem digital setiap saat.

03

Red & Blue Team: Dua tim kunci yang bekerja sama menguji dan memperkuat pertahanan keamanan organisasi.

6

03

ANALOGI KEAMANAN SIBER

"Menjadi aman di dunia internet, sama halnya menjadi aman di dunia nyata"

7

04

ANCAMAN DALAM DUNIA SIBER

1. **Social Engineering**
2. **Exploitasi pada Kerentanan Sistem**
3. **Kebocoran Data**
4. **Malware**
5. **Insider Attack**
6. **Supply Chain Attack**
7. **AI-Powered Attack**

8

05 SOCIAL ENGINEERING

Social Engineering adalah teknik serangan siber yang memanfaatkan **manipulasi psikologis dan perilaku manusia** untuk memperoleh informasi, akses, keuntungan finansial, atau tindakan tertentu dari korban.

Berbeda dengan serangan yang secara langsung mengeksploitasi kerentanan teknis pada sistem, **social engineering mengeksploitasi faktor manusia (human factor), seperti kepercayaan, rasa takut, rasa ingin tahu, dan rasa urgensi.**

9

06 EKSPLOITASI KERENTANAN

Eksploitasi pada kerentanan sistem merupakan tindakan **memanfaatkan kelemahan pada aplikasi, sistem operasi, jaringan, konfigurasi, atau perangkat** untuk memperoleh akses atau menjalankan aktivitas yang tidak seharusnya.

10

07 PEMANFAATAN KEBOCORAN DATA

Kebocoran data (Data Breach/Data Leak) adalah kondisi ketika **informasi sensitif diakses, diperoleh, digunakan, atau disebarluaskan** oleh pihak yang tidak memiliki kewenangan.

Biasanya, data-data tersebut diperjualbelikan dalam sebuah forum Dark Web atau platform-platform tertentu pada Darkweb.

11

08 AI-POWER ATTACK

AI-Powered Attack merupakan serangan siber yang memanfaatkan teknologi Artificial Intelligence untuk **meningkatkan kecepatan, skala, otomatisasi, personalisasi, atau efektivitas serangan.**

AI dapat dimanfaatkan oleh attacker untuk meningkatkan berbagai tahapan serangan, mulai dari reconnaissance hingga social engineering.

12

09 MALWARE

Malware (Malicious Software) adalah perangkat lunak yang dirancang untuk melakukan aktivitas berbahaya terhadap sistem, perangkat, jaringan, atau data.

Malware dapat digunakan untuk **memperoleh akses, mencuri informasi, merusak sistem, memantau aktivitas pengguna, atau mempertahankan akses secara tersembunyi.**

13

10 INSIDER ATTACK

Insider Attack adalah serangan atau penyalahgunaan yang dilakukan oleh individu yang memiliki **akses sah terhadap sistem, jaringan, atau informasi organisasi**.

Ancaman insider **tidak selalu berasal dari karyawan yang berniat jahat**, namun ada juga yang mendapatkan **pengaruh dari Attacker**.

14

11

SUPPLY CHAIN

Supply Chain Attack adalah **serangan yang menargetkan pihak ketiga, vendor, software, library, layanan, atau komponen teknologi** yang digunakan oleh organisasi sebagai jalur untuk mencapai target utama.

Penyerang tidak harus menyerang organisasi secara langsung. Mereka dapat terlebih dahulu mengkompromikan pihak yang memiliki hubungan kepercayaan dengan organisasi.

15

16

12

APA ITU RED TEAM?

01 Menguji keamanan sistem melalui simulasi serangan nyata untuk mengidentifikasi celah sebelum pihak jahat menemukannya.

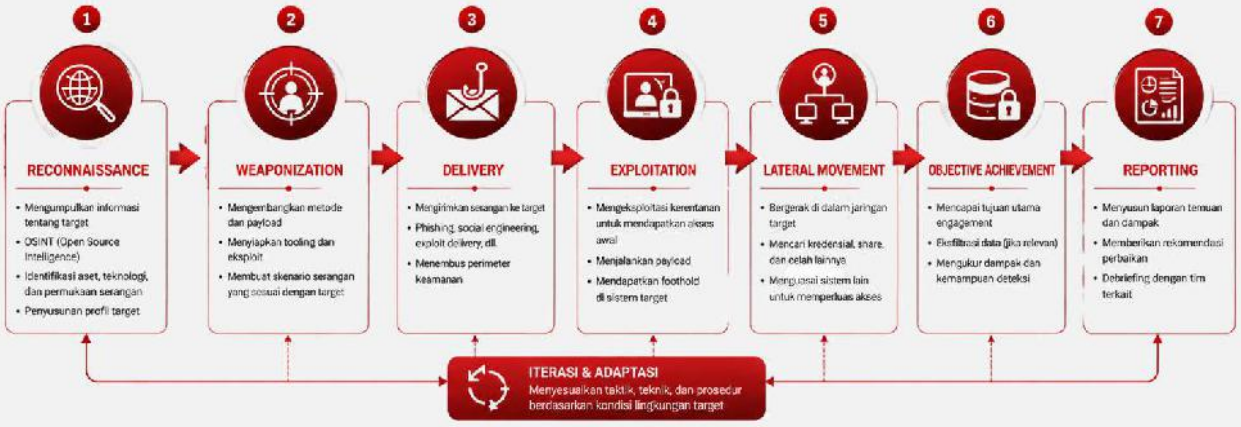
02 Mengeksploitasi kelemahan perangkat lunak, jaringan, dan manusia menggunakan teknik dan metode serangan yang terstruktur.

03 Meningkatkan kesiapan organisasi dalam menghadapi ancaman siber nyata dengan memberikan laporan temuan dan rekomendasi mitigasi.

17

13

METODE SERANGAN RED TEAM



18

ALAT & TEKNIK RED TEAM

14

Nessus® vulnerability scanner

metasploit®

SEARCHSPLOIT

NMAP

Ffuf

NUCLEI

BURPSUITE

CRACKMAP

GOPHISH

19

20

DARI SERANGAN KE PERTAHANAN: BLUE TEAM

15

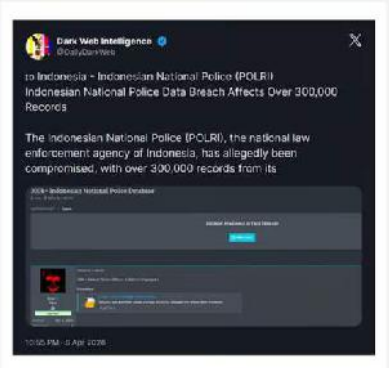
[redacted]ami bagaimana red team mengidentifikasi dan mengeksploitasi celah keamanan, kini saatnya beralih ke sisi pertahanan. Blue team hadir sebagai garda terdepan dalam melindungi sistem dan infrastruktur digital dari ancaman nyata.

Strategi pertahanan yang kuat dimulai dari pemahaman mendalam tentang metode serangan yang digunakan oleh red team.

21

BAGAIMANA STATUS KEAMANAN KITA SAAT INI?

16



Kasus Insiden Siber 2026

22

APA ITU BLUE TEAM?

17

BLUE TEAM ADALAH TIM PERTAHANAN KEAMANAN SIBER YANG BERTUGAS MELINDUNGI SISTEM DAN INFRASTRUKTUR ORGANISASI. MEREKA BERFOKUS PADA DETEKSI DINI, PENCEGAHAN, DAN RESPONS CEPAT TERHADAP ANCAMAN SIBER YANG TERUS BERKEMBANG.

Tim khusus yang melindungi aset digital organisasi.

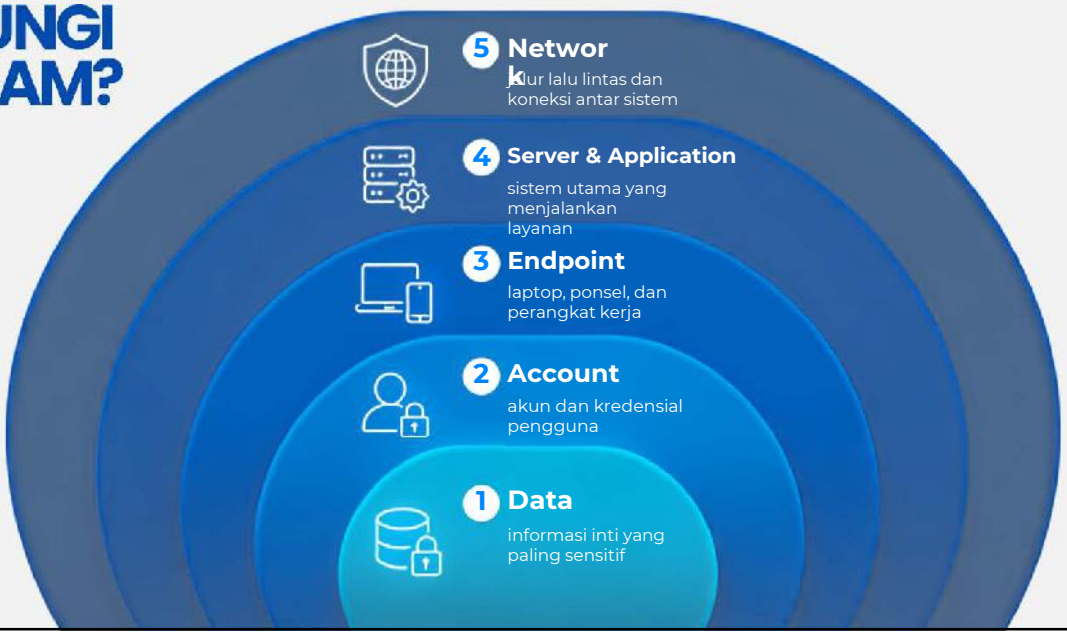
Mendeteksi dan mencegah ancaman siber secara proaktif.

Merespons insiden dengan cepat dan efektif.

23

APA YANG SEBENARNYA DILINDUNGI BLUE TEAM?

18



24

Incident Selesai ≠ Pekerjaan Selesai

SETELAH INSIDEN SELESAI

19

1. **FIND THE CAUSE** — Cari penyebab
2. **FIX** — Perbaiki kelemahan
3. **LEARN** — Evaluasi respons
4. **IMPROVE** — Perkuat pertahanan

Contoh:
MFA diterapkan, sistem di-patch, hak akses diperbaiki, monitoring ditingkatkan.

Tujuan kita bukan hanya menyelesaikan insiden,
tetapi mencegahnya terjadi lagi dan menjadi lebih kuat setiap hari.

25

FUNGSI UTAMA BLUE TEAM

BLUE TEAM MEMILIKI TANGGUNG JAWAB UTAMA DALAM MENJAGA KEAMANAN SISTEM TEKNOLOGI ORGANISASI SECARA BERKELANJUTAN

20

01 Pemantauan Keamanan Jaringan 24/7
Memantau lalu lintas jaringan secara terus-menerus untuk mendeteksi aktivitas mencurigakan.

02 Analisis Ancaman & Investigasi Insiden
Menganalisis ancaman siber dan menginvestigasi insiden keamanan secara mendalam.

03 Pengelolaan Patch & Kerentanan
Memastikan sistem selalu diperbarui dan kerentanan ditangani sebelum dieksploitasi.

04 Pengujian & Peningkatan Pertahanan
Menguji efektivitas sistem pertahanan dan terus meningkatkan postur keamanan organisasi.

26

TEKNIK PERTAHANAN

21

BLUE TEAM MENERAPKAN BERBAGAI TEKNIK PERTAHANAN BERLAPIS UNTUK MENDETEKSI, MENCEGAH, DAN MERESPONS ANCAMAN SIBER SECARA EFEKTIF.

STRATEGI INI DIRANCANG UNTUK MELINDUNGI ASET DIGITAL ORGANISASI MAUPUN INDIVIDU DARI SERANGAN YANG SEMAKIN CANGGIH.

- Deteksi Intrusi IDS/IPS
- Enkripsi Data & Komunikasi
- Manajemen Akses & Autentikasi
- Pelatihan Kesadaran Keamanan

27

TOOLS YANG DIGUNAKAN BLUE TEAM

22

- SIEM
- FIREWALL
- TOOLS FORENSIK
- INTELIJEN ANCAMAN
- EDR/XDR
- DLL

28

23

STRATEGI PERTAHANAN BLUE TEAM

01 Penggunaan sistem deteksi dan respons otomatis (IDS/IPS) untuk mitigasi ancaman.

02 Pendekatan proaktif: antisipasi dan pencegahan sebelum serangan terjadi pada sistem.

03 Pemantauan jaringan secara real-time untuk mendeteksi anomali dan ancaman sejak dini.

04 Penerapan patch dan update keamanan secara berkala untuk menutup celah pada sistem.

05 Pelatihan kesadaran keamanan siber bagi seluruh pengguna dan staf organisasi.

29

MEMBANGUN RESILIENSI ORGANISASI

24

Strategi keamanan berlapis da[illegible] respons insiden adalah fondas[illegible] ketahanan siber. Organisasi yang proaktif mampu mendeteksi, merespons, dan memulihkan diri dari ancaman dengan jauh lebih cepat dan efisien.

- **Terapkan strategi keamanan berlapis untuk perlindungan maksimal.**
- **70% organisasi dengan Blue Team proaktif kurangi waktu pemulihan hingga 50%.**
- **Kesiapan respons insiden mempercepat pemulihan dan meminimalkan kerugian.**

30

STUDI KASUS:
RESPONS BLUE TEAM

25

Sebuah organisasi pemerintahan diserang ransomware yang mengenkripsi 80% data operasional. Blue Team berhasil mendeteksi anomali dalam 12 menit, mengisolasi sistem yang terinfeksi, dan memulihkan operasional secara penuh dalam 4 jam tanpa membayar tebusan.

01 **Deteksi dini melalui SIEM menghentikan penyebaran ransomware.**

02 **Isolasi jaringan cepat mencegah enkripsi data lebih lanjut.**

08 **Pemulihan sistem dari backup bersih dalam waktu kurang dari 4 jam.**

31

PERAN INDIVIDU DALAM KEAMANAN SIBER

26

Kata Sandi Kuat

Gunakan kata sandi yang kuat, unik, dan berbeda untuk setiap akun agar lebih aman.

Pembaruan Perangkat Lunak

Perbarui perangkat lunak secara rutin untuk menutup celah keamanan dan kerentanan.

Waspada Phishing

Waspadai email dan pesan mencurigakan yang mencoba mencuri informasi pribadi Anda.

Autentikasi Dua Faktor (2FA)

Aktifkan 2FA pada semua akun penting untuk lapisan perlindungan tambahan yang lebih kuat.

32

KESADARAN & TATA KELOLA KEAMANAN INFORMASI

27

1. KESADARAN KEAMANAN SIBER

Fondasi perilaku aman bagi organisasi dan individu.

- Pelatihan keamanan siber secara rutin dan berkelanjutan
- Simulasi phishing untuk menguji kewaspadaan karyawan
- Penggunaan kata sandi kuat dan autentikasi dua faktor (2FA)
- Pelaporan insiden keamanan dengan cepat dan tepat

2. TATA KELOLA KEAMANAN INFORMASI

Kerangka kerja yang andal untuk pengelolaan keamanan.

- Kebijakan dan prosedur keamanan yang jelas
- Peran dan tanggung jawab yang tegas di setiap level
- Manajemen risiko yang terstruktur dan proaktif
- Kepatuhan terhadap standar dan regulasi (ISO 27001, dll.)
- Audit dan evaluasi keamanan secara berkala
- Perbaikan berkelanjutan (continuous improvement)

Awareness + Governance = Resiliensi Keamanan yang Lebih Kuat

33

KESADARAN KEAMANAN SIBER

28

APA ITU SECURITY AWARENESS?

Pemahaman dan kebiasaan setiap individu untuk mengenali, mencegah, dan merespons ancaman siber.

Mengapa Penting?

- Organisasi: Mengurangi risiko kebocoran data & serangan rekayasa sosial
- Individu: Melindungi identitas digital, finansial, dan privasi
- 95% insiden keamanan melibatkan human error (IBM/Verizon DBIR)

MEMBANGUN KEBIASAAN AMAN SEHARI-HARI

- Pelatihan keamanan siber rutin & berkelanjutan (minimal per kuartal)
- Simulasi phishing berkala untuk mengukur kewaspadaan
- Selalu verifikasi pengirim & tautan sebelum klik
- Gunakan kata sandi unik + aktifkan 2FA di semua akun
- Pembaruan perangkat lunak & patch secara tepat waktu
- Laporkan insiden atau aktivitas mencurigakan dengan segera

INSIGHT

Awareness bukan sekadar pelatihan satu kali. Ini adalah budaya — kebiasaan yang terus diperkuat melalui pengulangan, simulasi, dan feedback loop yang konsisten.

FAKTA

Organisasi dengan program awareness matang mengalami penurunan insiden phishing hingga 70% dalam 12 bulan pertama. (SANS Security Awareness Report)

Awareness menurunkan risiko human error & memperkuat resiliensi organisasi maupun individu

Awareness + Governance = Resiliensi Keamanan yang Lebih Kuat

34

GOVERANCE KEAMANAN INFORMASI

29

APA ITU GOVERNANCE KEAMANAN INFORMASI?

Kerangka kerja strategis yang memastikan keputusan keamanan konsisten, terdokumentasi, terukur, dan dapat diaudit di seluruh organisasi.

Mengapa Penting?

- Memberikan arah dan akuntabilitas dalam pengelolaan risiko siber
- Memastikan kepatuhan terhadap regulasi & standar (ISO 27001, NIST, dll.)
- Menyelaraskan strategi keamanan dengan tujuan bisnis organisasi

KOMPONEN UTAMA GOVERNANCE

- Kebijakan & prosedur keamanan yang terdokumentasi
- Pembagian peran & tanggung jawab (RACI) di setiap level
- Manajemen risiko terstruktur dan proaktif
- Klasifikasi aset dan data berdasarkan sensitivitas
- Kontrol akses berbasis least privilege & need-to-know
- Audit, monitoring, dan kepatuhan berkelanjutan
- Perbaikan berkelanjutan (Plan-Do-Check-Act)

PRINSIP KUNCI

Governance yang baik memastikan setiap keputusan keamanan bersifat konsisten, terdokumentasi, dan dapat diaudit — bukan bergantung pada individu tertentu.

CONTOH KASUS

Perusahaan tanpa governance jelas mengalami breach karena akses admin tidak direviu selama 2 tahun. Dengan governance: reviu akses berkala, segregation of duties, dan audit trail mencegah hal serupa.

Governance = Fondasi keputusan keamanan yang konsisten, terukur, dan dapat dipertanggungjawabkan

Awareness + Governance = Resiliensi Keamanan yang Lebih Kuat

35

CONTOH KASUS: AWARENESS & GOVERNANCE

30

SEBELUM: Tanpa Program Awareness & Governance

- **Karyawan menerima email phishing palsu — 40% mengklik tautan berbahaya**
- **Tidak ada prosedur pelaporan insiden yang jelas**
- **Akses admin tidak pernah direviu — mantan karyawan masih punya akses**
- **Tidak ada kebijakan MFA/2FA — kredensial mudah dikompromikan**
- **Dampak: Kebocoran data 10.000 pelanggan, denda regulasi, reputasi rusak**

SESUDAH: Dengan Awareness + Governance Terintegrasi

- **Pelatihan awareness rutin per kuartal + simulasi phishing bulanan**
- **Kebijakan pelaporan insiden < 1 jam dengan eskalasi otomatis**
- **Reviu akses berkala (quarterly) + prinsip least privilege**
- **MFA/2FA wajib untuk semua sistem kritis**
- **Tata kelola jelas: RACI, approval workflow, audit trail lengkap**
- **Hasil: Klik phishing turun 85%, waktu respons insiden < 30 menit**

PELAJARAN UTAMA

- ✓ **Awareness tanpa governance = perilaku baik tanpa sistem pendukung**
- ✓ **Governance tanpa awareness = aturan bagus yang tidak dijalankan**
- ✓ **Kombinasi keduanya = resiliensi nyata & terukur**
- ✓ **Respon lebih cepat, risiko lebih rendah, keputusan konsisten**

DAMPAK TERUKUR

- Insiden phishing berhasil: -85%
- Waktu deteksi & respons: dari 72 jam → < 30 menit
- Kepatuhan audit ISO 27001: tercapai dalam 6 bulan
- Kepercayaan stakeholder: meningkat signifikan

Awareness + Governance = Respon Lebih Cepat | Risiko Lebih Rendah | Keputusan Keamanan Konsisten

Awareness + Governance = Resiliensi Keamanan yang Lebih Kuat

36

TERIMA KASIH

SUROSOWAN CYBER

diskominfo kota Cimahi

37