Raka Aditya Pratama | Cybersecurity Engineer | Spesialis Keamanan Jaringan dan Cloud

Jl. Cikini Raya No. 45, Jakarta Pusat, DKI Jakarta, Indonesia, 10330
+62 812-3456-7890 • raka.pratama@cybermail.id • https://www.rakaaditya.id
@rakaadityapratama • @rakaaditya

Informasi Dasar

Cybersecurity Engineer dengan pengalaman lebih dari 6 tahun dalam merancang, mengoperasikan, dan meningkatkan kontrol keamanan untuk lingkungan enterprise, cloud, dan aplikasi web. Terampil dalam threat hunting, incident response, pengujian penetrasi, serta hardening infrastruktur dan identitas. Fokus pada pengurangan risiko siber secara terukur melalui otomasi, kolaborasi lintas tim, dan kepatuhan terhadap standar ISO 27001, NIST CSF, dan PCI DSS. Berpengalaman memimpin investigasi insiden, membangun runbook respons, dan melatih tim internal dalam praktik keamanan yang aman.

Pendidikan

Universitas Indonesia **https://www.ui.ac.id**

Sarjana, Ilmu Komputer, Nilai: 3.72 *Agu 2013–Jul 2017*

- Menguasai dasar-dasar keamanan informasi, kriptografi, dan forensik digital melalui perkuliahan dan proyek laboratorium.
- Mengembangkan aplikasi berbasis web dan melakukan analisis kerentanan dasar sebagai bagian dari tugas akhir.
- Aktif dalam kelompok studi keamanan siber kampus dan membantu penyelenggaraan workshop Capture The Flag.

Mata Kuliah: Keamanan Informasi, Jaringan Komputer, Kriptografi, Sistem Operasi, Basis Data, Pemrograman Lanjut, Forensik Digital, Arsitektur Perangkat Lunak

Pengalaman Kerja

PT Nusantara Cyber Solutions **https://www.nusantaracyber.co.id**

Senior Cybersecurity Engineer *Mar 2022–Sekarang*

- Memimpin tim blue team dalam pemantauan keamanan 24/7, threat hunting, dan investigasi insiden untuk klien enterprise di sektor keuangan dan energi.
- Merancang dan mengimplementasikan otomasi incident response berbasis SOAR yang memangkas waktu triase alert hingga 40%.
- Melakukan pengujian penetrasi aplikasi web, API, dan infrastruktur cloud serta menyusun rekomendasi remediasi yang dapat ditindaklanjuti.
- Mengembangkan runbook, playbook, dan matriks eskalasi insiden yang selaras dengan NIST CSF dan ISO 27001.
- Melatih analis junior dan tim TI klien mengenai praktik secure configuration, phishing awareness, dan manajemen kerentanan.

Kata Kunci: Incident Response, Threat Hunting, SIEM, ISO 27001

PT Bank Digital Sentosa **https://www.bankdigitalsentosa.co.id**

Cybersecurity Engineer *Jun 2019–Feb 2022*

- Mengelola dan menyempurnakan aturan deteksi pada SIEM, mendukung monitoring transaksi digital dan aktivitas pengguna berisiko.
- Melakukan vulnerability assessment dan penetration testing pada aplikasi mobile banking, portal web, dan layanan API.
- Berkontribusi dalam program kepatuhan PCI DSS dan ISO 27001, termasuk pengumpulan bukti audit dan remediasi temuan.
- Mengimplementasikan network segmentation, hardening server, dan kontrol akses berbasis prinsip least privilege.
- Bekerja sama dengan tim fraud dan risiko untuk mendeteksi serta merespons indikasi penipuan siber secara cepat.

Kata Kunci: PCI DSS, Vulnerability Assessment, Network Security, Mobile Security

PT Teknologi Aman Indonesia **https://www.teknologiaman.id**

Security Operations Analyst *Agu 2017–Mei 2019*

- Memantau alert keamanan dari SIEM, firewall, IDS/IPS, dan endpoint protection untuk mendeteksi aktivitas mencurigakan.
- Melakukan triase, klasifikasi, dan eskalasi insiden sesuai SLA serta mendokumentasikan temuan dalam tiket investigasi.
- Membantu analisis malware dasar, pengumpulan bukti digital, dan penyusunan laporan insiden mingguan.
- Mengotomatisasi tugas pengumpulan log dan enrichment IOC menggunakan skrip Python dan API keamanan.
- Mendukung penyusunan prosedur operasional keamanan dan knowledge base untuk tim SOC.

Kata Kunci: SOC, IDS/IPS, Malware Analysis, Python

Bahasa

Indonesia: Bahasa Ibu / Bilingual — **Kata Kunci**: Bahasa ibu

Inggris: Tingkat Profesional Penuh — **Kata Kunci**: TOEFL iBT 105, IELTS 7.5

Keahlian

Keamanan Jaringan: Ahli — **Kata Kunci**: Firewall, IDS/IPS, VPN, Network Segmentation, Zero Trust

Pengujian Penetrasi: Mahir — **Kata Kunci**: Burp Suite, Metasploit, Nmap, OWASP Top 10, Kali Linux

Keamanan Cloud: Mahir — **Kata Kunci**: AWS Security Hub, IAM, Azure Defender, CSPM, Kubernetes Security

Incident Response: Ahli — **Kata Kunci**: SIEM, SOAR, Threat Hunting, Digital Forensics, Malware Analysis

Tata Kelola dan Kepatuhan: Mahir — **Kata Kunci**: ISO 27001, PCI DSS, NIST CSF, Risk Assessment, Audit

Penghargaan

Penghargaan Inovasi Keamanan Terbaik

PT Nusantara Cyber Solutions *Nov 2023*

Diberikan atas perancangan platform otomasi incident response yang mengurangi waktu deteksi dan respons insiden sebesar 40%.

Sertifikat

Certified Information Systems Security Professional (CISSP) **https://www.isc2.org/certifications/cissp**

ISC2 *Jun 2023*

Offensive Security Certified Professional (OSCP) **https://www.offsec.com/certifications/oscp/**

Offensive Security *Sep 2021*

AWS Certified Security - Specialty **https://aws.amazon.com/certification/certified-security-specialty/**

Amazon Web Services *Mar 2022*

Publikasi

Jurnal Keamanan Siber Indonesia **https://jurnal.keamanansiber.id/volume-7/no-1/d**

Deteksi Anomali Jaringan Menggunakan Pembelajaran Mesin untuk Lingkungan Cloud

- Membahas pendekatan deteksi anomali berbasis pembelajaran mesin untuk memantau lalu lintas jaringan cloud.
- Mengevaluasi performa model terhadap dataset lalu lintas normal dan serangan yang disimulasikan.
- Memberikan rekomendasi implementasi untuk tim keamanan yang mengelola lingkungan hybrid cloud.

Referensi

Dr. Intan Prameswari **+62 811-9876-5432**

Dosen Keamanan Informasi, Universitas Indonesia *intan.prameswari@ui.ac.id*

Raka menunjukkan kemampuan analisis keamanan yang kuat, etika kerja yang tinggi, dan kepemimpinan yang baik dalam proyek incident response. Ia mampu menghubungkan temuan teknis dengan kebutuhan risiko bisnis secara jelas.

Proyek

Platform Otomasi Incident Response **https://github.com/rakaaditya/ir-automation**

Platform internal untuk mengotomatisasi triase, enrichment, dan eskalasi alert keamanan. *Jan 2023–Okt 2023*

- Mengintegrasikan SIEM, threat intelligence, dan sistem tiket untuk mempercepat alur investigasi insiden.
- Menyediakan playbook otomatis untuk phishing, malware, dan akses tidak sah.
- Mengurangi waktu respons awal dari rata-rata 25 menit menjadi 15 menit.

Kata Kunci: Otomasi, SOAR, Threat Intelligence, Python

Pemindaian Kerentanan Aplikasi Web **https://github.com/rakaaditya/web-**

Alat pemindaian kerentanan aplikasi web untuk mendeteksi konfigurasi tidak aman dan celah umum. *Apr*

- Mengotomatisasi pemeriksaan header keamanan, cookie, dan konfigurasi TLS.
- Mendeteksi indikasi kerentanan OWASP Top 10 melalui pengujian non-destruktif.
- Menghasilkan laporan temuan yang dapat diekspor untuk kebutuhan remediasi dan audit.

Kata Kunci: OWASP, Web Security, Python, Automation

Minat

Keamanan Siber: Capture The Flag, Riset Kerentanan, Threat Intelligence

Kegiatan Luar Ruang: Mendaki, Bersepeda, Fotografi

Kegiatan Sukarela

Komunitas Keamanan Siber Indonesia **https://www.keamanansiber.id/komunitas**

Mentor Keamanan Aplikasi *Feb 2020–Sekarang*

- Membimbing peserta workshop tentang secure coding, pengujian penetrasi web, dan manajemen kerentanan.
- Membantu menyusun materi pelatihan praktis untuk pemula dan profesional TI.
- Berperan sebagai juri dan fasilitator dalam kompetisi Capture The Flag tingkat nasional.