Chief Security Officer (CSO)

Tujuan utama:
Menjamin **keamanan data, platform, dan infrastruktur cloud** 32Inside secara menyeluruh, sekaligus menjaga kepatuhan terhadap standar industri dan regulasi.

□□ Fungsi Utama:

- Menetapkan **strategi keamanan siber** perusahaan, baik untuk platform internal maupun layanan pelanggan.
- Memastikan penerapan **security by design** dalam setiap proyek dan produk.
- Mengawasi **operasional keamanan 24x7**, dari deteksi ancaman hingga mitigasi insiden.
- Menjaga **kepatuhan terhadap standar keamanan** (ISO 27001, SOC 2, PDPA, dan sejenisnya).
- Mengembangkan **kultur keamanan** di seluruh lini organisasi.
- Berkolaborasi erat dengan CTO (infrastruktur) dan CSDO (operasi) untuk keamanan menyeluruh.

□□ Security Operations Division

1. **SOC Manager**

Fokus: Mengelola operasi Security Operation Center (SOC) untuk monitoring, deteksi, dan respon insiden keamanan secara real-time.

Tugas Detail:

- Memimpin tim SOC 24x7 yang melakukan **monitoring keamanan infrastruktur cloud dan jaringan** (OpenStack, Kubernetes, Ceph, internal apps).
- Membangun dan memelihara **SIEM (Security Information and Event Management)** untuk korelasi log, alerting, dan dashboard insiden.
- Menyusun **runbook incident response** untuk berbagai jenis serangan (DDoS, brute force, privilege escalation, data exfiltration, dsb).
- Melakukan **threat hunting** proaktif berdasarkan IOC (Indicator of Compromise) dan intel terbaru.

- Menetapkan prioritas penanganan insiden berdasarkan severity & business impact.
- Mengatur eskalasi ke Security Engineering atau Platform tim jika perlu tindakan teknis lanjut.
- Melakukan post-incident review dan menghasilkan **Root Cause Analysis (RCA)**.
- Menyusun laporan **MTTD (Mean Time to Detect)** dan **MTTR (Mean Time to Respond)** untuk evaluasi efektivitas SOC.
- Melatih tim operasi dan teknis terkait prosedur keamanan dan pelaporan insiden.

Tools biasa digunakan:

- **SIEM:** Wazuh, Graylog, ELK Stack, Splunk (Enterprise), Security Onion
- **Threat Intelligence:** MISP, OpenCTI, AlienVault OTX
- **Monitoring & Detection:** Suricata, Zeek (Bro), CrowdSec, Fail2Ban, OSSEC
- **Incident Management:** TheHive, Cortex, RTIR, Jira Security

---

□□ Security Engineering & Compliance Division

2. **Security Engineering Manager**

Fokus: membangun dan mengelola sistem keamanan teknis (hardening, encryption, vulnerability management, IAM) di seluruh platform.

Tugas Detail:

- Merancang kebijakan dan prosedur **server hardening** untuk OpenStack, Kubernetes, dan sistem internal.
- Melakukan **vulnerability assessment & remediation** berkala menggunakan scanner otomatis dan manual verification.
- Mengelola **encryption system** (data-at-rest dan data-in-transit), termasuk TLS certificate lifecycle, disk encryption, dan secret management.
- Mengelola **IAM (Identity and Access Management)** untuk semua platform — Role-Based Access Control (RBAC), MFA, least privilege principle.
- Mengawasi integrasi dengan **Key Management Service (KMS)** atau Vault system untuk penyimpanan kredensial.
- Bekerjasama dengan DevOps & Platform Services untuk menerapkan **secure CI/CD pipeline**.
- Menyusun kebijakan patch management, serta memastikan **patch compliance rate** tinggi.
- Melakukan **security testing** terhadap layanan SaaS dan API internal.

- Melakukan **collaboration dengan SOC** untuk menutup gap keamanan yang terdeteksi dari threat monitoring.
- Menulis dan memperbarui **security guideline dan best practice documentation** internal.

Tools biasa digunakan:

- **Vulnerability Scanning:** OpenVAS, Nessus, Trivy, Clair, Nmap, Lynis
- **Hardening:** CIS Benchmark tools, Ansible hardening roles, auditd
- **IAM:** Keycloak, Vault, FreeIPA, OpenLDAP, JumpCloud
- **Encryption & Secrets:** HashiCorp Vault, GnuPG, OpenSSL, cert-manager
- **Testing:** OWASP ZAP, Burp Suite, Nikto, Metasploit (for red teaming)

---

3. **Compliance Manager**

Fokus: memastikan bahwa seluruh proses, sistem, dan dokumentasi perusahaan **mematuhi standar keamanan dan regulasi** yang berlaku.

Tugas Detail:

- Menyusun dan mengelola **ISMS (Information Security Management System)** sesuai ISO/IEC 27001:2022.
- Memastikan seluruh divisi menjalankan **security policy dan control** yang sesuai dengan framework (ISO27001, SOC 2, PDPA, GDPR).
- Menyusun dan memperbarui **dokumentasi keamanan**, termasuk risk register, asset inventory, dan Statement of Applicability (SoA).
- Mengkoordinasikan **audit internal dan eksternal** bersama auditor independen.
- Melakukan **gap analysis** dan perbaikan temuan hasil audit (non-conformance closure).
- Menyusun **Business Impact Assessment (BIA)** dan mendukung tim Resilience (CSDO) untuk DRP/BCP.
- Melakukan training internal tentang **security awareness dan data protection** untuk seluruh karyawan.
- Mengelola **vendor security assessment** untuk partner atau supplier yang terhubung dengan platform.
- Menyiapkan **compliance report dan evidence log** untuk keperluan audit pelanggan enterprise.
- Berkoordinasi dengan Legal dan CPCO untuk kebijakan privasi dan HR compliance.

Tools biasa digunakan:

- **GRC & Audit Tools:** ISO Manager, Conformio, AuditBoard, Jira GRC, Excel templates
- **Documentation & Workflow:** Confluence, Notion, SharePoint
- **Awareness & Training:** KnowBe4, LMS internal, Google Forms (quiz)
- **Risk Register:** Excel-based tracker atau open-source GRC (eramba, SimpleRisk)

Revision #1
Created 9 November 2025 01:28:10 by Kapak Maut
Updated 25 June 2026 20:28:53 by Kapak Maut