Dokumen Spesifikasi Produk

# Contoso CipherGuard Sentinel X7

# 1. Gambaran Umum Produk

## 1.1 Pengantar

Contoso CipherGuard Sentinel X7 adalah produk keamanan canggih dan tangguh yang direkayasa dengan cermat untuk membentengi infrastruktur jaringan komputer terhadap spektrum ancaman dan kerentanan. Dokumen ini mempelajari seluk-beluk spesifikasi teknis, fitur, dan fungsionalitas Contoso CipherGuard Sentinel X7 .

## 1.2 Fitur Utama

* **Perlindungan Firewall:** Menggunakan firewall inspeksi yang memiliki kondisi, Contoso CipherGuard Sentinel X7 menggunakan teknik inspeksi paket yang mendalam. Ini memeriksa dan menganalisis paket jaringan di lapisan aplikasi, memberikan kontrol terperinci atas aliran data. Firewall secara dinamis menyesuaikan seperangkat aturannya berdasarkan konteks jaringan yang berkembang, mengurangi risiko yang terkait dengan serangan lapisan aplikasi.
* **Sistem Deteksi dan Pencegahan Intrusi (IDPS):** Didukung oleh algoritma pembelajaran mesin, IDPS kami terus memantau pola dan anomali lalu lintas jaringan. Ini memanfaatkan deteksi berbasis tanda tangan, deteksi anomali, dan analisis heuristik untuk mengidentifikasi dan menggagalkan potensi ancaman. Sistem ini menggunakan umpan inteligensi ancaman, memastikannya tetap diperbarui dengan pola serangan terbaru yang diketahui.
* **Dukungan Virtual Private Network (VPN):** Contoso CipherGuard Sentinel X7 mendukung protokol VPN standar industri, seperti IPsec dan OpenVPN. Ini memfasilitasi komunikasi yang aman melalui jaringan publik dengan mengenkripsi data saat transit. Modul VPN menggunakan algoritma kriptografi tingkat lanjut, termasuk AES-256, memastikan saluran komunikasi yang kuat dan aman untuk pengguna jarak jauh dan kantor cabang.
* **Keamanan Titik Akhir:** Menggunakan pendekatan pertahanan berlapis, modul keamanan titik akhir kami menggabungkan antivirus, anti-malware, dan kemampuan pencegahan intrusi berbasis host. Ini melakukan analisis perilaku real-time dan pemindaian heuristik, memastikan deteksi proaktif dan penahanan aktivitas berbahaya. Selain itu, ini terintegrasi dengan platform inteligensi ancaman untuk respons cepat terhadap ancaman yang muncul.
* **Pengelogan dan Pemantauan:** Subsistem pengelogan dan pemantauan menangkap data komprehensif tentang aktivitas jaringan. Ini termasuk log terperinci tentang pola lalu lintas, peristiwa autentikasi pengguna, dan pelanggaran kebijakan keamanan. Terintegrasi dengan SIEM (Security Information and Event Management), fitur ini memudahkan pemantauan dan analisis terpusat, memberdayakan administrator keamanan untuk merespons potensi insiden keamanan dengan cepat.
* **Autentikasi Pengguna dan Kontrol Akses**: Contoso CipherGuard Sentinel X7 mendukung mekanisme autentikasi multifaktor (MFA), termasuk autentikasi biometrik dan integrasi kartu pintar. Kebijakan kontrol akses didasarkan pada peran pengguna, memanfaatkan integrasi LDAP dan Direktori Aktif. Penegakan kebijakan dinamis memastikan bahwa hanya pengguna yang berwenang yang mendapatkan akses ke sumber daya sensitif.

# 2. Spesifikasi Teknis

## 2.1 Persyaratan Perangkat Keras

* **Prosesor:** Quad-core 2,5 GHz atau lebih tinggi dengan dukungan akselerasi perangkat keras
* **RAM:** Minimum 16 GB, ECC (Kode Koreksi Kesalahan) direkomendasikan
* **Penyimpanan:** Minimum 200 GB, SSD untuk performa optimal
* **Kartu Antarmuka Jaringan (NIC):** Ethernet Gigabit Ganda dengan dukungan untuk bingkai jumbo

## 2.2 Persyaratan Perangkat Lunak

* **Sistem Operasi:** Kompatibel dengan Windows Server 2019 ke atas, CentOS 8 atau setara
* **Database:** PostgreSQL 13 untuk penyimpanan data, dioptimalkan untuk pengindeksan berkinerja tinggi
* **Pembaruan Keamanan:** Pembaruan otomatis untuk umpan inteligensi ancaman dan patch keamanan reguler

## 2.3 Kompatibilitas Jaringan

* **Protokol:** dukungan TCP/IP, UDP, ICMP, IPv6
* **Integrasi:** Integrasi mulus dengan protokol perutean BGP dan OSPF
* **Kompatibilitas:** Interoperabilitas dengan Cisco, Juniper, dan vendor jaringan utama lainnya

# 3. Rencana Penerapan

## 3.1 Langkah-Langkah Penerapan

1. **Penilaian Pra-Penerapan:** Melakukan penilaian kerentanan jaringan yang komprehensif, termasuk pengujian penetrasi dan analisis risiko.
2. **Penginstalan:** Terapkan Contoso CipherGuard Sentinel X7 pada server khusus atau komputer virtual, memastikan pemanfaatan perangkat keras dan alokasi sumber daya yang optimal.
3. **Konfigurasi:** Menyesuaikan kebijakan keamanan, kontrol akses, dan aturan firewall berdasarkan persyaratan organisasi. Menyempurnakan parameter deteksi intrusi untuk akurasi maksimum.
4. **Pengujian:** Menjalankan rencana pengujian menyeluruh, termasuk skenario simulasi serangan dan pengujian beban, untuk memvalidasi efektivitas dan kinerja solusi.
5. **Pelatihan:** Menyediakan sesi pelatihan mendalam untuk personel TI, yang mencakup operasi sehari-hari, prosedur respons insiden, dan tugas pemeliharaan.

## 3.2 Pemeliharaan dan Dukungan

* **Pembaruan Reguler:** Contoso menjamin pembaruan berkelanjutan untuk produk, menggabungkan inteligensi ancaman terbaru dan peningkatan keamanan.
* **Dukungan Teknis:** Contoso menyediakan tim dukungan 24/7 khusus untuk memastikan bantuan cepat untuk masalah teknis atau pertanyaan yang terkait dengan Contoso CipherGuard Sentinel X7 .