DIREKTORAT JENDERAL KEKAYAAN INTELEKTUAL
KEMENTERIAN HUKUM & HAK ASASI MANUSIA R.I.

PENGAMANAN DATA
DIREKTORAT JENDERAL KEKAYAAN INTELEKTUAL

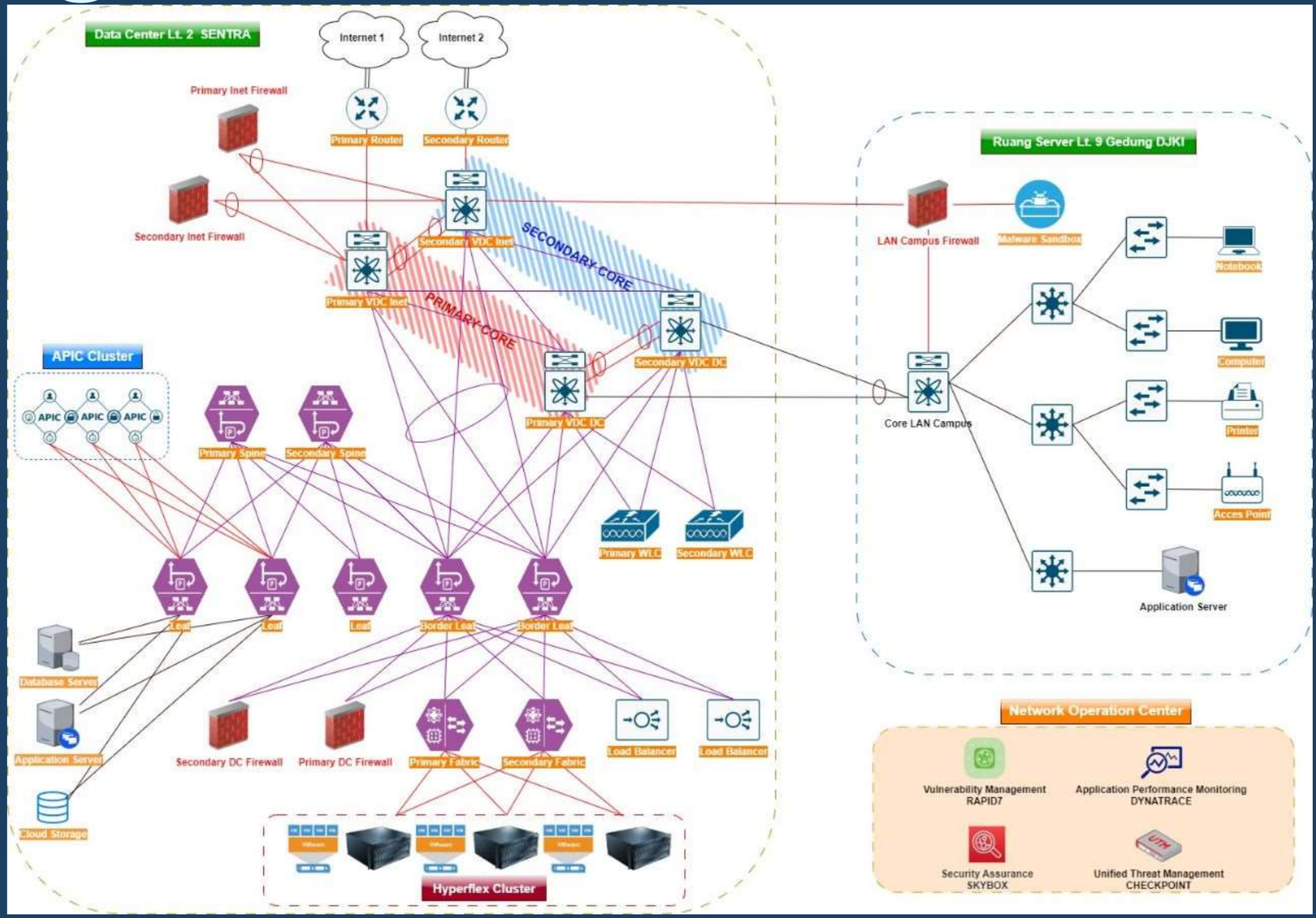
1. NOC

Direktorat Jenderal Kekayaan Intelektual memiliki NOC
NETWORK OPERATION CENTER
berlokasi di Gedung DJKI Lantai 9

Terdiri dari:

1. Video Wall Display
2. Vulnerability Management RAPID7
3. Aplikasi Performance Monitoring DYNATRACE
4. Network Assurance Scanner SkyBox SECURITY
5. Unified Threat Management CHECKPOINT

Topologi NOC



2. Perangkat SOC DJKI Sebelumnya

Perangkat Pendukung SOC antara lain:

1. NGFW Fire Power. Merupakan sekuriti jaringan yang melindungi End User dan Aplikasi yang terdapat di dalam jaringan DJKI
2. Anti Virus Kapersky. Merupakan anti virus yang terinstal di dalam PC dan server DJKI.
3. Forti Mail. Perangkat filtering spam e-mail resmi dgip.go.id, agar reputasi dari domain DJKI terjaga.

3. SOC (security operation center)

SOC – Security Operation Center yang dimiliki Direktorat Jenderal Kekayaan Intelektual tahun 2023 , merupakan perangkat security yang berfungsi mengamankan seluruh jaringan aplikasi layanan kekayaan intelektual maupun data pada Direktorat Jenderal Kekayaan Intelektual.

Perangkat Pendukung SOC antara lain:

1. Threat Intelligent

Melakukan monitoring yang ada di Dark Web terkait informasi mencakup data DJKI dan sebagai umpan informasi untuk threat intelligent terkait cyber attack.

Mampu secara akurat melakukan crawling, menganalisis, dan menginterpretasikan data dari banyak sumber untuk mengidentifikasi kredensial yang bocor dan data rahasia lainnya. memberikan insight dan konteks yang dapat ditindaklanjuti tentang teknologi yang berpotensi rentan untuk mempercepat proses penilaian dan verifikasi. secara proaktif memantau pemetaan ancaman phishing dan memberikan statistik dan serangan phishing global terbaru dari internet.

Menganalisis jutaan domain setiap hari di sebagian besar pendaftar domain utama untuk mendeteksi domain berbahaya atau mirip yang menargetkan merek tertentu dan seluruh jaringan bisnis.

2. Content Delivery Network (CDN)

Perlindungan Aplikasi DJKI berbasis Web dari Ancaman anti Ddos dan Web Aplication Firewall.

3. Network Detection and Response (NDR)

Berfungsi sebagai monitoring terhadap anomali yang berjalan disisi network atau jaringan DJKI. Mempunyai kemampuan dapat mendeteksi serangan SOL injection, dapat monitoring server dan infrastruktur jaringan dengan metode out of band, memantau aktivitas mencurigakan perubahan peran pengguna, akses tidak sah, dan lainnya.

Memiliki kemampuan untuk mengumpulkan informasi aset dan informasi flow jaringan, dapat melakukan capture network data dan hanya mengirimkan relevant data ke processor untuk analisa.

Mempunyai fitur Machine Learning -Intrusion Detection System dengan kemampuan dapat mendeteksi serangan DDOS, Worm outbreak, Port Scan, Brute Force, serangan dari internal ke internal, dan serangan dari eksternal ke internal

4. SIEM (Security Information Event Management), UEBA (User Behaviour Analytic).
   Melakukan Analisis Log secara automat parsing (memilah data log secara otomatis) terkait serangan secara internal maupun eksternal disisi network djki.

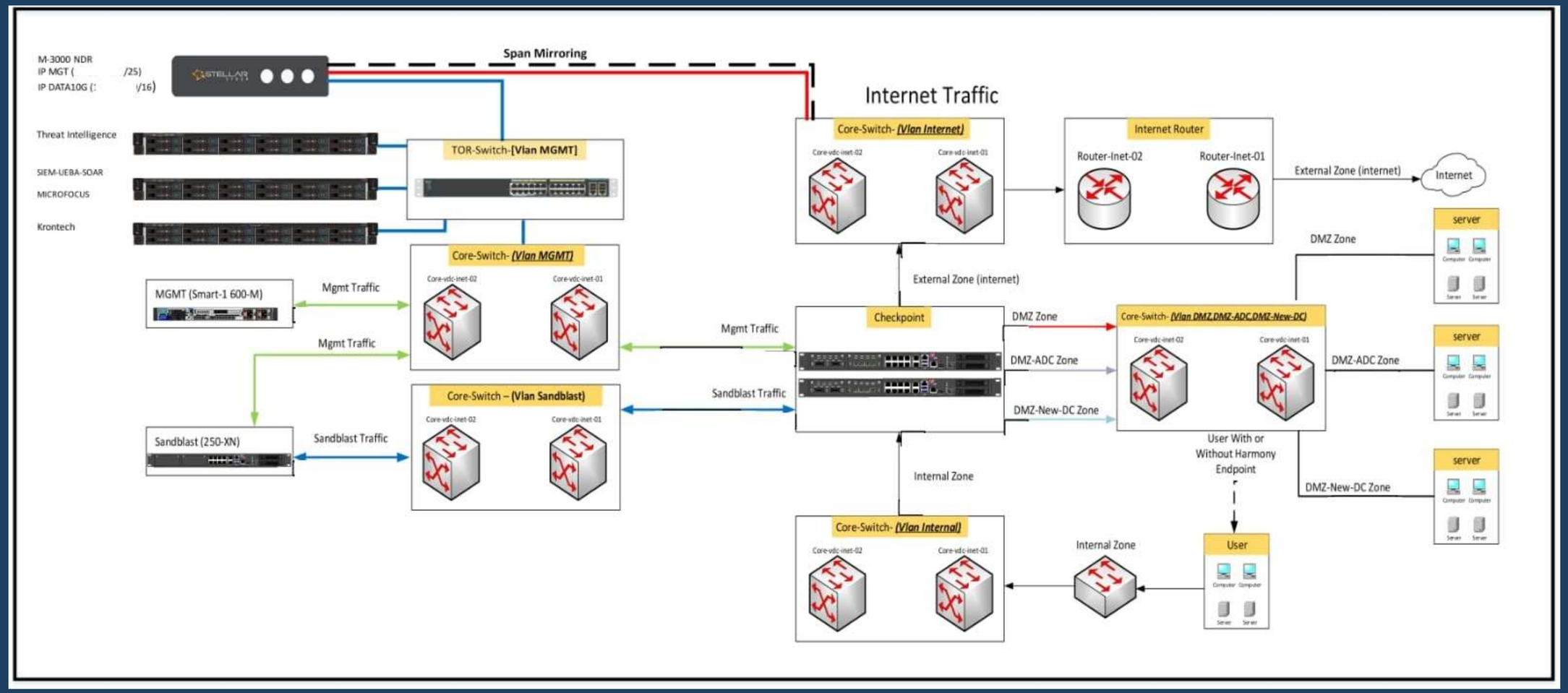
5. Privilage Access Management (PAM)
   PAM bekerja melalui proses, dan teknologi, serta memberi visibilitas tentang siapa yang menggunakan akun dengan hak istimewa dan apa yang dilakukan saat mereka masuk.

6. Next Generation Firewall
   Untuk Menfiltering atau Sebagai Gateway Jarigaan dan Policy yang ada di DJKI

7. Endpoint Detection and Response (anti virus)
   Untuk scaning dan mengfiltering firus, malware, spam yang terdapat di jaringan DJKI khususnya untuk perangkat end user (pegawai) dan server

8. Silverport
   Silverport adalah solusi autentikasi multi-faktor yang memungkinkan Anda untuk melindungi data sensitif dengan menggunakan cara autentikasi yang lebih canggih di atas autentikasi nama pengguna dan kata sandi biasa. Dengan Autentikasi Lanjutan (Advanced Authentication), Anda dapat mengautentikasi pada berbagai platform dengan menggunakan berbagai jenis autentikator seperti Sidik Jari, Kartu, dan OTP. Autentikasi Lanjutan menyediakan kerangka kerja autentikasi tunggal yang memastikan akses aman ke semua perangkat Anda dengan administrasi minimal

Topologi SOC Ditjen KI



4. Pengembangan SOC DJKI

1. Perlunya pengelola SDM Profesional untuk membantu tugas dan fungsi dari perangkat yang dimiliki oleh DJKI dan mendeteksi kerentanan dalam aplikasi, sistem, atau infrastruktur DJKI dan melewati keamanan sistem untuk mengidentifikasi potensi pelanggaran dan ancaman data. Di antaranya melalui jasa EOS Engineering On Site.
2. Adanya training atau pelatihan tentang pengetahuan mengenai Certified Ethical Hacking dimana agar dapat menilai keamanan sistem komputer dengan mencari kelemahan dan kerentanan dalam sistem target
3. Penambahan perangkat-perangkat dan lisensi untuk meningkatkan performa SOC yang dimiliki oleh DJKI, terdiri dari : Lisensi Cisco Secure Network Analytic, perangkat DNS Domain Name Server Security, Monitoring Tools Network.

DIREKTORAT JENDERAL KEKAYAAN INTELEKTUAL
KEMENTERIAN HUKUM & HAK ASASI MANUSIA R.I.

Terima kasih!