PELAKSANAAN INSTALASI PERISIAN NEXT-GENERATION ANTIVIRUS (NGAV) SECARA BERPERINGKAT

Bahagian Keselamatan Siber

Mac 2024

Agenda

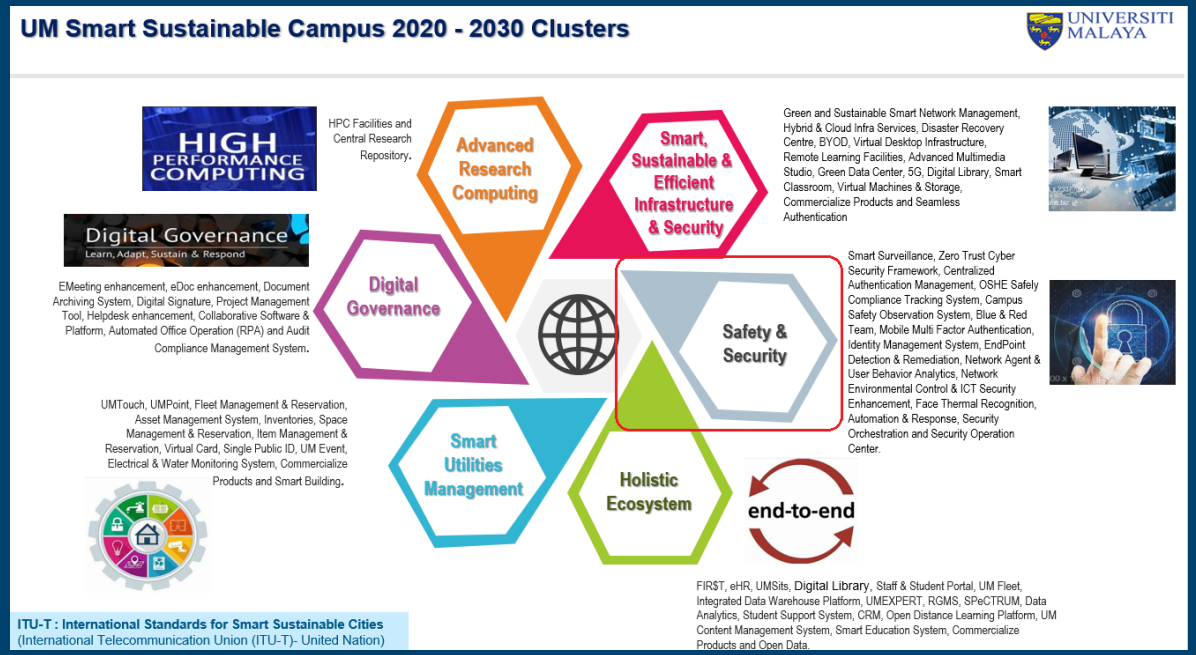
- Pengenalan
- Next Generation Antivirus (NGAV)
- Fungsi & Kelebihan NGAV
- Implikasi
- Isu Keselamatan Siber
- Pasukan Projek & Instalasi
- Aktiviti Pelaksanaan Instalasi
- Pasca Pelaksanaan
- Kesan Selepas Pelaksanaan
- Pelaporan
- Jadual Pelaksanaan

Pengenalan

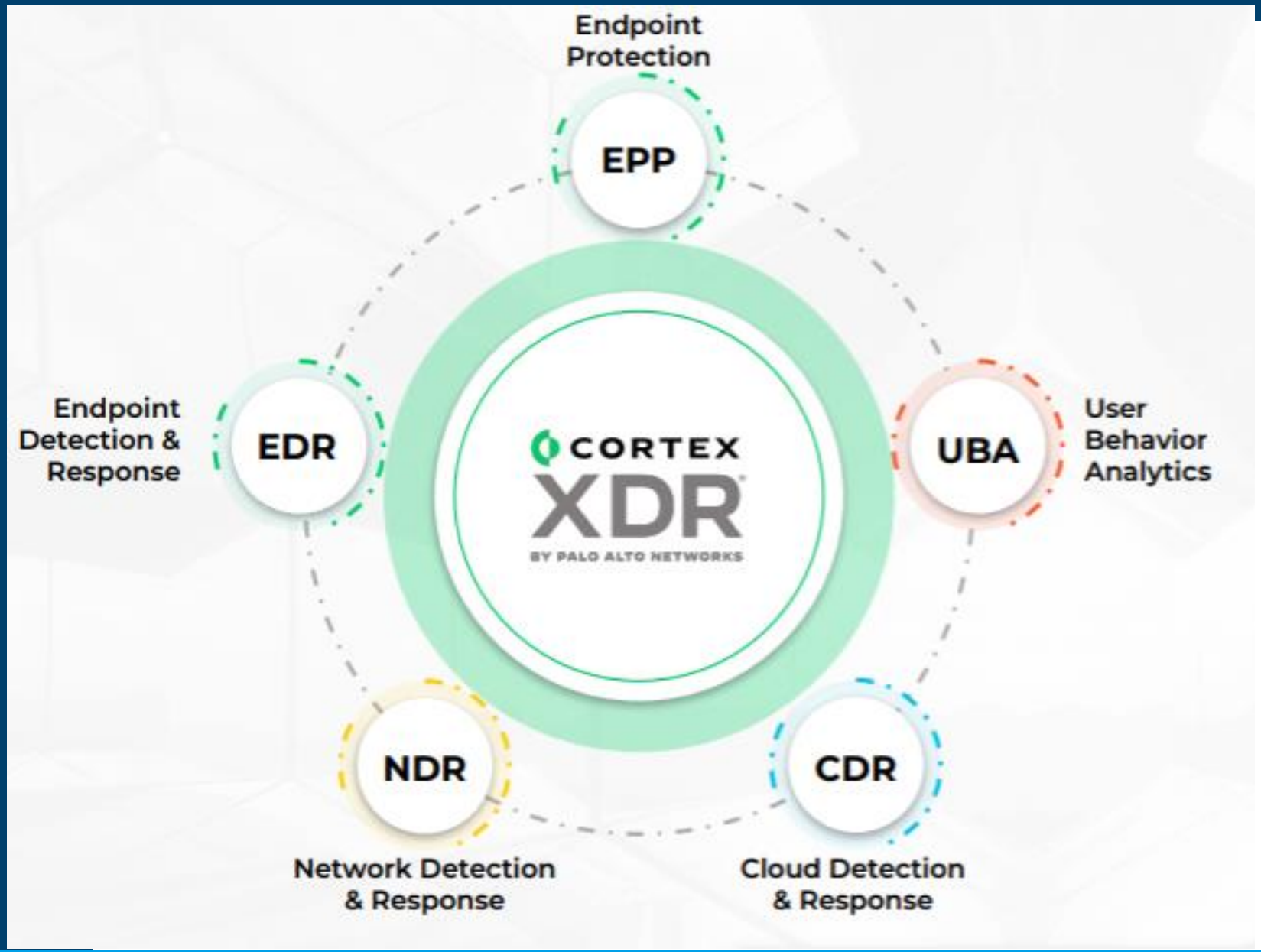
Projek Unified EndPoint Security Platform & Incident Response System:

- Salah satu inisiatif UM Smart Sustainable & Efficient Infrastructure

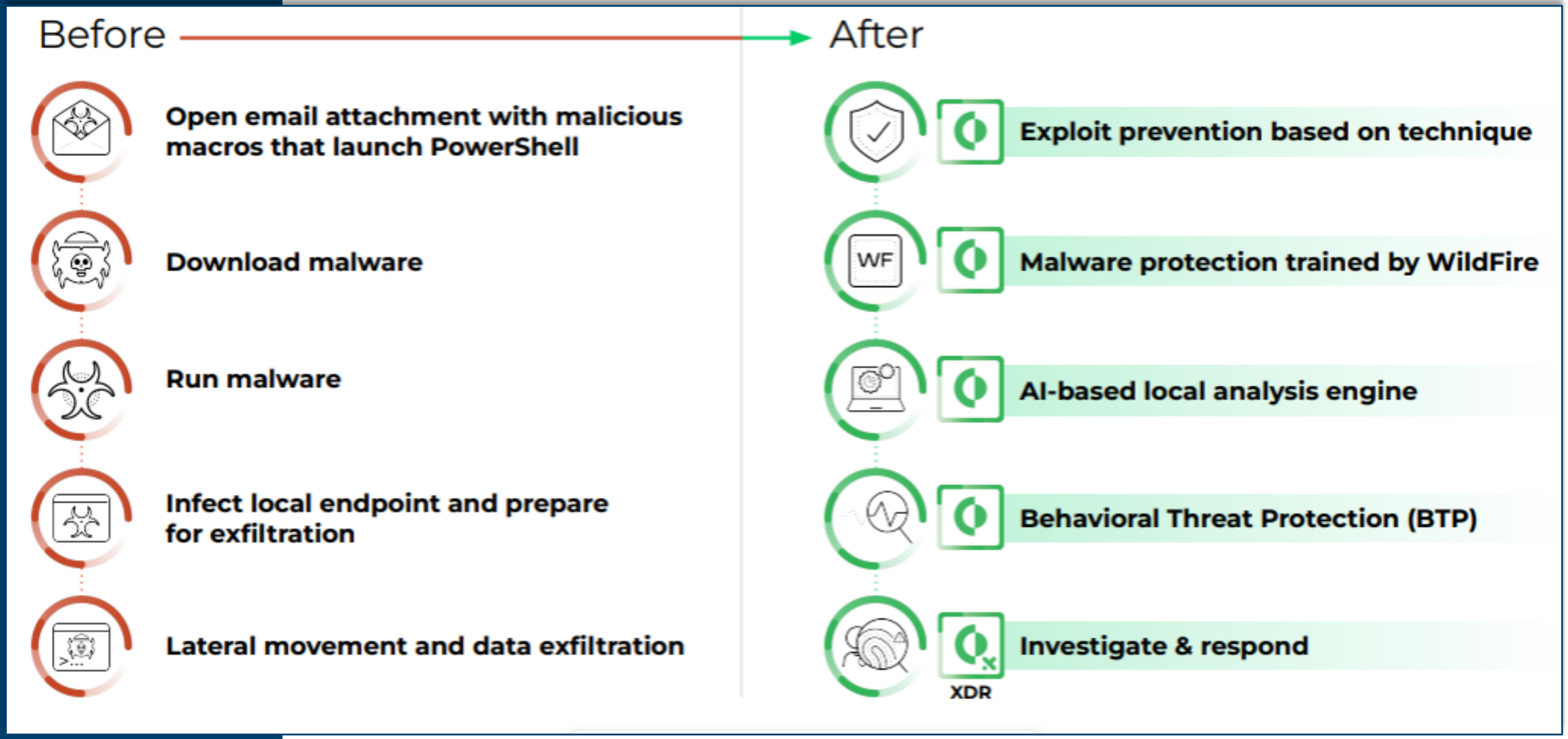
Cluster : Safety & Security



Next Generation Antivirus (NGAV)



Perbezaan Next Gen AV dgn Tradisional AV



Fungsi dan Kelebihan NGAV

Menyekat malware, ransomware, eksploit & serangan tanpa fail

Melindungi endpoint dengan kawalan peranti, firewall dan disk encryption

Menggunapakai machine learning & User and Entity Behavior Analytics (UEBA) pada keselamatan data

Mengenalpasti ancaman dan melakukan tindak balas dengan Artificial Intelligence-driven analytics

Implikasi

Menghadapi risiko ancaman penggodaman

Risiko Endpoint yang dijangkiti yang membuat serangan secara l*ateral movement* tidak dapat dikawal

Mengurangkan masa min untuk respons (MTTR-mean time to response)

Risiko serangan siber & ketirisan data (spt. data penyelidikan, data pengajaran, data rasmi) akan meningkat

Menyukarkan proses pemulihan ancaman kerana asset tidak dapat dikenal pasti lokasi dan jenis ancaman yang terlibat

Perlindungan tidak menyeluruh dan boleh menjadi punca ruangan masuk ancaman pada rangkaian

Isu Keselamatan Siber

2.4 Juta

Purata 2.4 juta sebulan bilangan malicious queries menunjukkan bilangan endpoint yg dijangkiti adalah tinggi

12,000

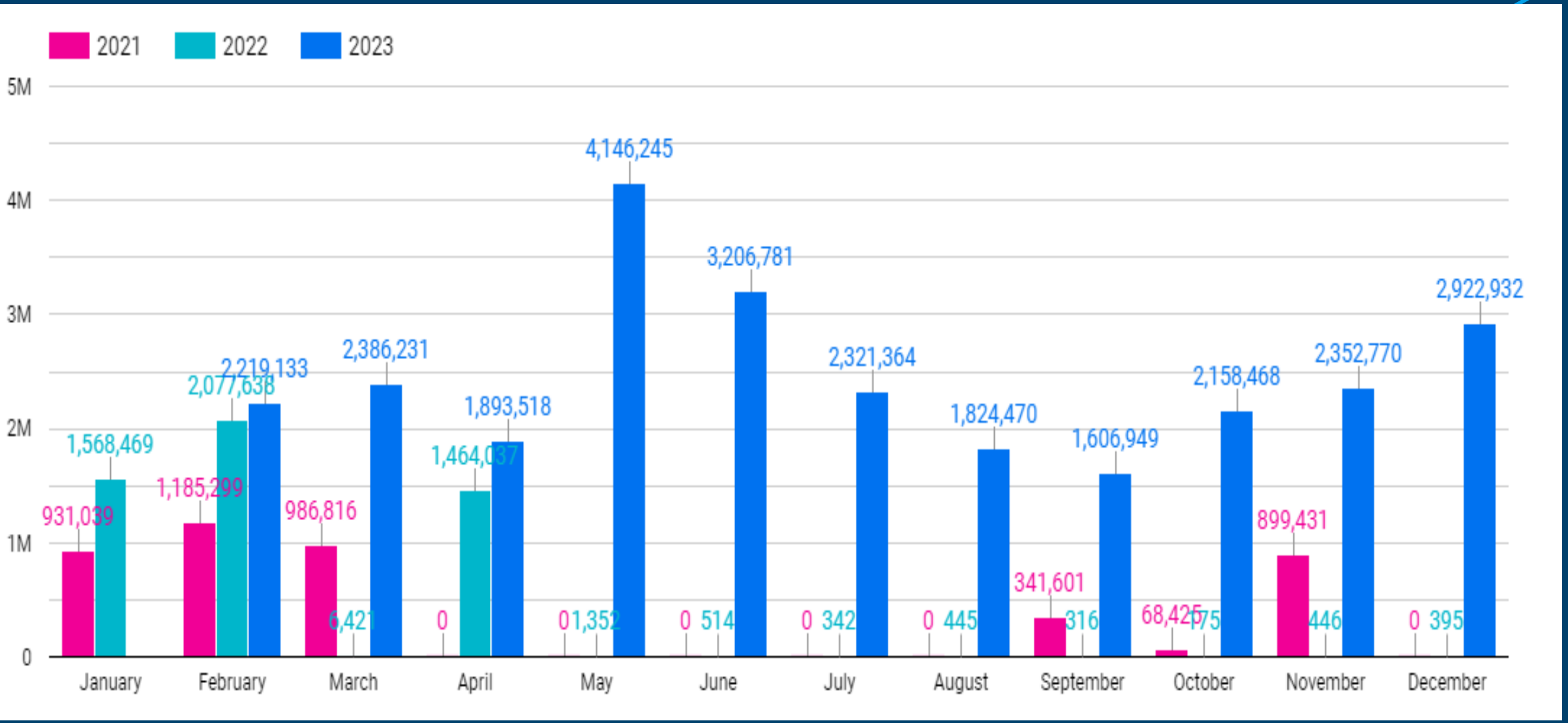
- Akaun pengguna UM telah dikompromi (compromised credential) dan dijual di Dark Web
- Penggodam menggunakan kombinasi akaun & kata laluan ini untuk menembusi akaun-akaun lain (credential stuffing attack)

* Statistik Analisa Keselamatan Siber 2023

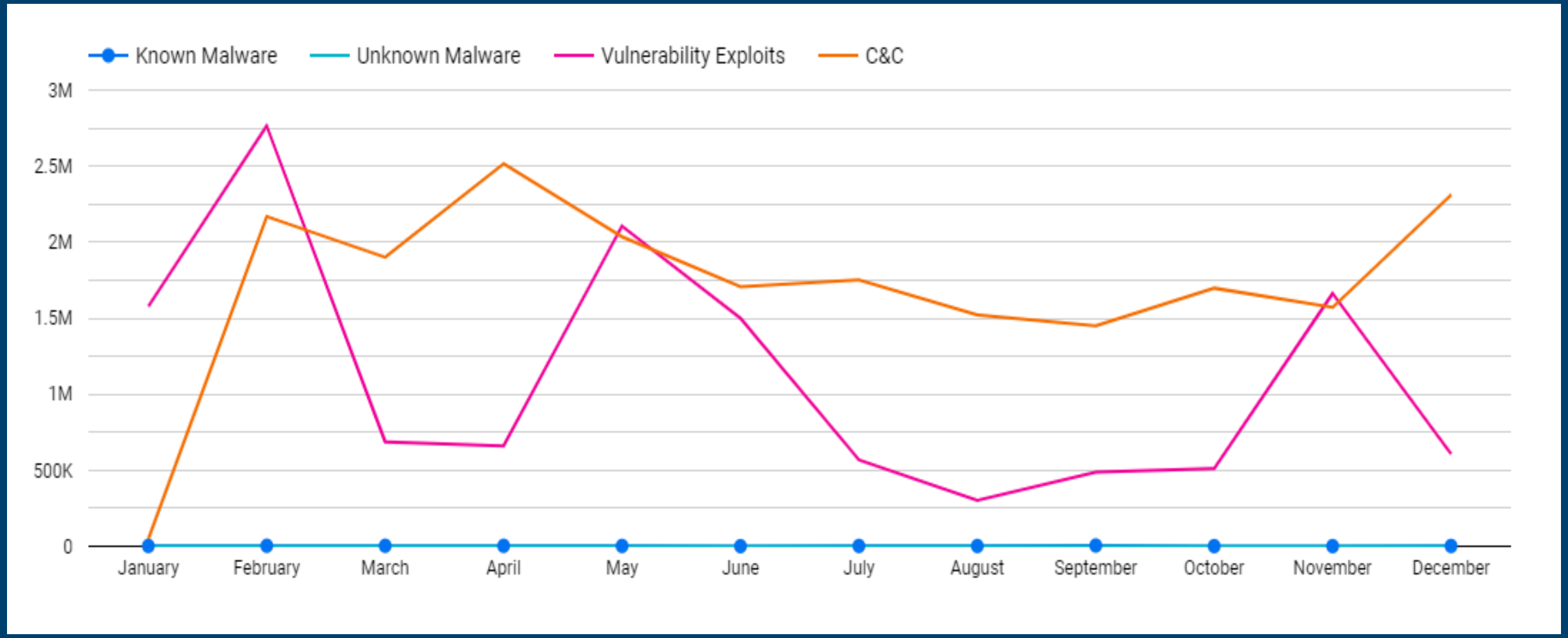
Isu Keselamatan Siber

- Proses pengesanan perkakasan yang dijangkiti dilaksanakan secara manual dan mengambil masa yang lama untuk dibersihkan/dipulihkan
- Amaran dari Security Operation Center (SOC) diuruskan secara manual.
- Penetapan keutamaan sukar untuk dilaksanakan

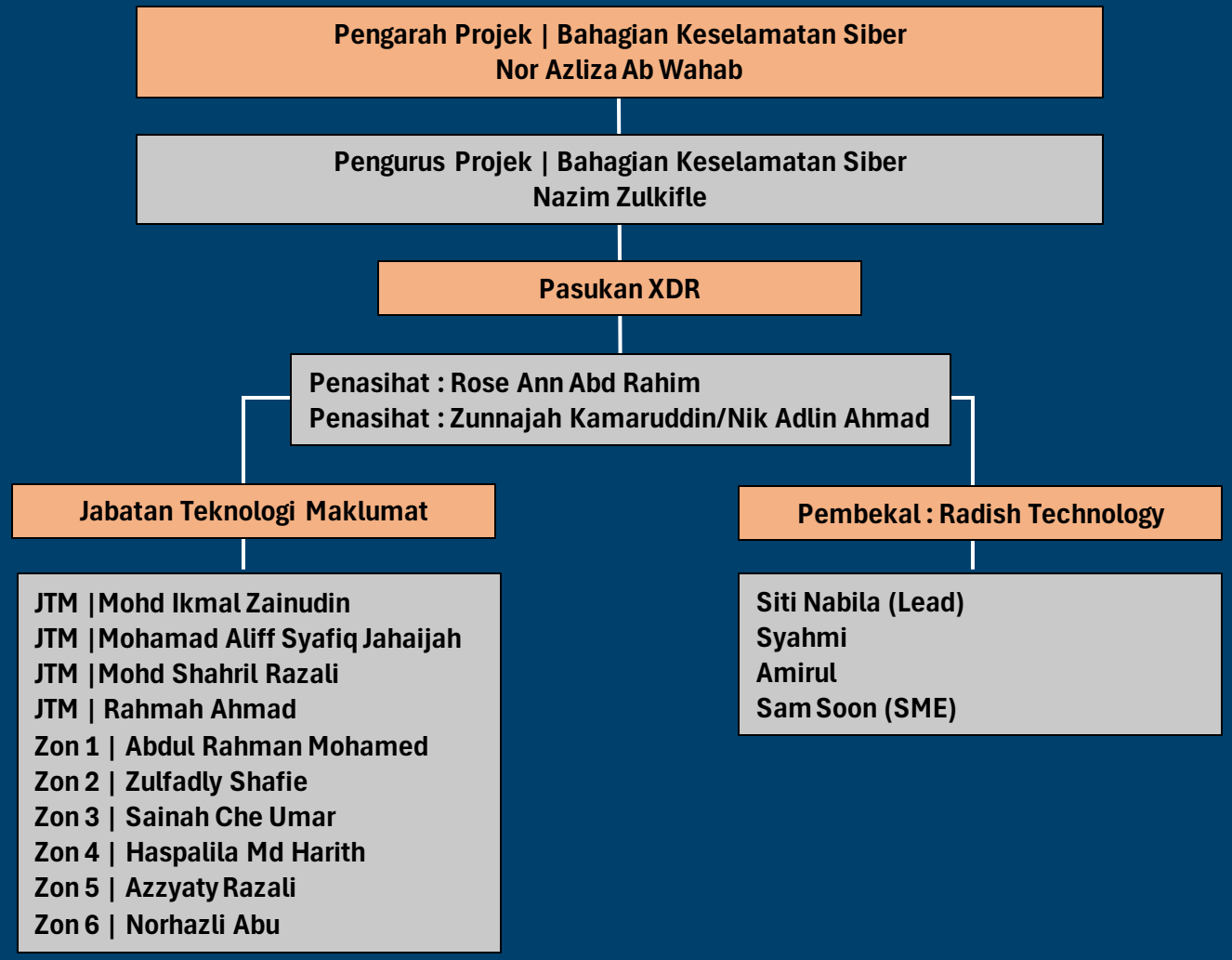
Statistik Bilangan Ancaman Siber 2021-2023



Statistik Bilangan Ancaman Siber Mengikut Kategori 2023



Pasukan Projek



Pasukan Instalasi

Pasukan instalasi terdiri:

1. Wakil Keselamatan Siber (1)
2. Wakil Pengkomputeran (1)
3. Wakil Staf F di PTj/ Wakil PTj (1 atau 2)
4. Wakil Pembekal (2)

* Wakil PTj akan mengiringi pasukan bagi tujuan instalasi.

Aktiviti Pelaksanaan Instalasi Berperingkat

* Instalasi hanya akan dilaksanakan semasa kehadiran pengguna di lokasi.

Aktiviti instalasi:

1. Membuat semakan sistem operasi
2. Membuat semakan sekiranya terdapat sebarang antivirus lain
3. Melaksanakan nyahpasang (uninstall) antivirus sedia ada jika ada
4. Melaksanakan instalasi ngav Cortex XDR
5. Melaksanakan semakan ‘heartbeat’ kepada XDR Cloud

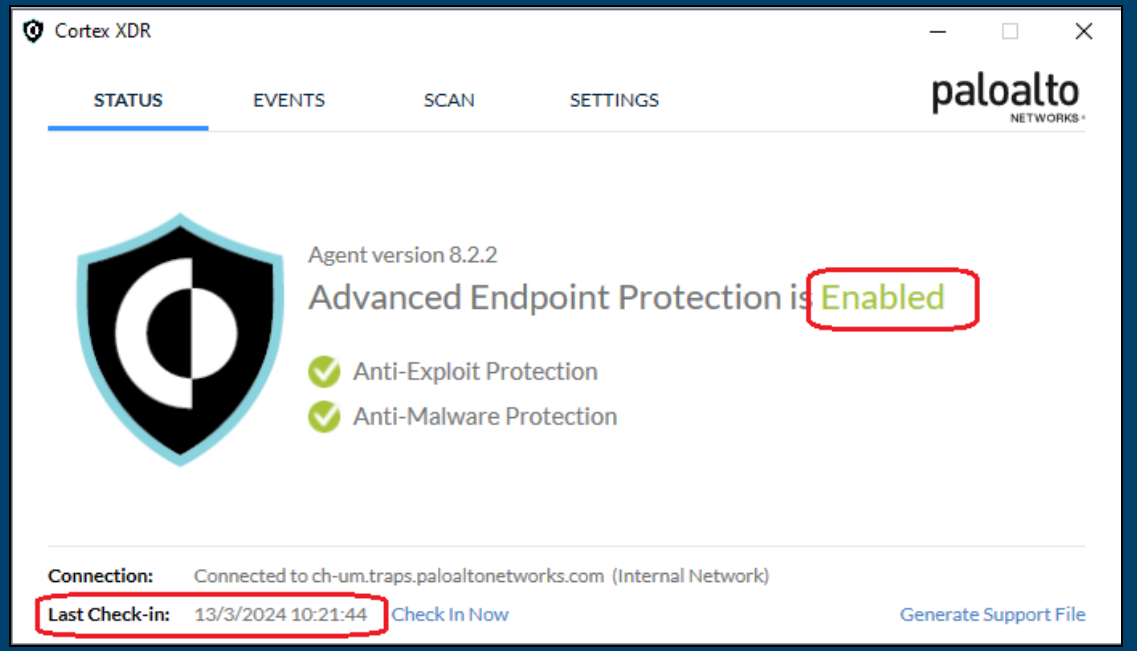
Persediaan Sebelum Pelaksanaan

1. Membuat Windows & Software Update pc yang terlibat
2. Maklumkan segera kepada Pasukan JTM jika terdapat sebarang acara/perkara yang boleh menyebabkan aktiviti pelaksanaan di PTj tertangguh.

Selepas Instalasi NGAV(Agen Cortex XDR)

- Ikon  akan tertera di bawah kanan pc/laptop

- Untuk semakan sama ada NGAV adalah terkini, klik kanan ikon. Console akan terpapar



Kesan Selepas Instalasi

Tiada kesan kepada User Experience

- Cortex XDR hanya memantau sekiranya terdapat ancaman penggodam/serangan virus dan melaksanakan tindakan pencegahan sekiranya ada

Cortex XDR TIDAK menyemak/menyimpan maklumat peribadi pengguna

- Hanya mengenalpasti fail atau aplikasi yang dilayari.

Nota Tambahan

1. Hanya pc milik UM dan BYOD sahaja yang terlibat.
2. Sekiranya pemilik mempunyai lebih dari 1 pc, pc utama sahaja yang akan dipilih.
3. Sekiranya pemilik tiada semasa sesi instalasi, pemilik / wakil ICT boleh hubungi pasukan JTM utk dapatkan NGAV ini.
4. Perlu install semula NGAV sekiranya pc diformat.

Pelaporan

Sebarang pertanyaan lanjut mengenai perkara ini boleh hubungi pegawai di Jabatan Teknologi Maklumat seperti berikut:

Staf Bhg.Infrastruktur ICT:

Encik Mohamad Aliff Syafiq Bin Jahaijah

Emel: aliff_syafiq@um.edu.my

Telefon: 603-79676720

Staf Bhg. Keselamatan Siber:

Encik Mohd Ikmal Bin Zainuddin

Emel: ictsecurity@um.edu.my

Telefon: 603-79677153

Jadual Pelaksanaan dan Taklimat

Jadual Pelaksanaan ada di UMPortal => News

https://portal.um.edu.my/

Bertajuk : Jadual Taklimat & Pelaksanaan Kerja-Kerja Instalasi Perisian Next Gen Anti-Virus

Link terus : https://portal.um.edu.my/news.php?id=1333

Jadual Pelaksanaan

Tarikh	Lokasi	Bilangan Komputer	Pegawai Dihubungi
21/03/2024 – 29/03/2024	Fakulti Kejuruteraan	569	Pn. Sainah Che Umar sainah@um.edu.my
	Akademi Pengajian Melayu		Pn. Noormei Azura Zakaria mieyy66@um.edu.my
	Pusat Asasi Sains		En. Mohd Hasri Bin Che Ros hasri86@um.edu.my
	Bangunan Peperiksaan		Cik Noor Shyahira Binti Adnan shyahira@um.edu.my
1/04/2024 - 8/04/2024	Fakulti Sains Sukan & Sains Eksesais	615	En. Adib Aqmal Bin Khalid adibaqmal@um.edu.my
	Akademi Pengajian Islam		En. Norhazli Abu lirock@um.edu.my
	Fakulti Bahasa & Linguistik		Pn. Syazwani binti Nuru Mohamad syazwani@um.edu.my
	Institut Pengurusan dan Perkhidmatan Penyelidikan		En. Rohaizad Adenan aizadadenan@um.edu.my
	Institut Asia-Eropah Institut Pengajian China Institut Pengajian Termaju		En. Alif Farkhan Bin Mohd Sharif aliffarkhan@um.edu.my

Jadual Pelaksanaan

Tarikh	Lokasi	Bilangan Komputer	Pegawai Dihubungi
22/04/2024 – 29/04/2024	Perpustakaan Utama	620	Pn. Marzulaila Johari marzulaila@um.edu.my
	Perpustakaan Zaaba		En. Muhammad Afiq bin Zulku aafiqz@um.edu.my
	Kompleks Perdanasiswa		En. Alif Farkhan Bin Mohd Sharif aliffarkhan@um.edu.my
	Fakulti Perniagaan dan Ekonomi		En. Zulfadly bin Shafie zulf5@um.edu.my En. Mohd Farhan Ibrahim frhan@um.edu.my
	Fakulti Sains Komputer dan Teknologi Maklumat		Pn. Azzyaty Binti Razali azzyaty@um.edu.my En. Mohd Farhan Bin Abdul Rahman farhan.rahman@um.edu.my

Jadual Pelaksanaan

Tarikh	Lokasi	Bilangan Komputer	Pegawai Dihubungi
2/05/2024 – 10/05/2024	Fakulti Sains	606	En. Mohamad Nazmi Bin Mohd Nazri mnazmi@um.edu.my En. Salim Shah Bin Kader Batcha salimshah@um.edu.my
	Fakulti Pendidikan		En. Mohd Hakimin Bin Sharuddin hakimie@um.edu.my
13/05/2024 – 21/05/2024	Fakulti Sastera dan Sains Sosial Klinik Kesihatan	785	En. Mohd Kamaruzaman Bin Hasan kamaruzaman@um.edu.my En. Mohamad Ramadan Bin Ramle adan@um.edu.my
	Bangunan Canseleri		En. Muhammad Fadhil Abd Razak fadhil85@um.edu.my Pn. Rosliza bt Sapiei rosliza@um.edu.my
	Bangunan HIR		En. Sutian bin Mohd Zin mr_yan83@um.edu.my
	Fakulti Seni Kreatif		En. Mohd Ridhwan Mohd Ezad rihdwan08@um.edu.my Cik Sumazutia Baharuddin le12@um.edu.my

Jadual Pelaksanaan

Tarikh	Lokasi	Bilangan Komputer	Pegawai Dihubungi
23/05/2024 – 31/05/2024	Fakulti Farmasi	616	En. Mohd Asni Mohamed asni@um.edu.my
	Fakulti Pergigian		En. Abdul Qayum Bohari qayum@um.edu.my Pn. Siti Zubaidah Makhtar jue86@um.edu.my
4/06/2024 – 14/06/2024	Fakulti Perubatan	844	Pn. Nurul Faezah Pamuji nurulfaezah@um.edu.my En. Muhammad Syimir Badri syimirbadri@um.edu.my
17/06/2024 – 21/06/2024	Jabatan Harta Benda Kolej – Kolej Kediaman Wisma R & D PALAPES	615	
	Fakulti Alam Bina		En. Mohd Annuar bin Ja'afar annuar@um.edu.my
	Fakulti Undang- undang		En. Mohd Fauzie Bin Pamuji fauzie@um.edu.my

Terima Kasih