



METHOD OF PROCEDURE

Instalasi EDR Cybereason

Kontrol Dokumen

Document Name : MOP – Instalasi EDR Cybereason

Revision	Prepared by	Approved By
1.0	Telkomsigma	

1 Pendahuluan

1.1 Tujuan

Tujuan dari dokumen ini adalah untuk melakukan instalasi EDR Cybereason di Tenant PDNS. Fokus perhatian adalah memastikan kesuksesan proses instalasi.

Dokumen ini juga akan memberikan rincian informasi cara konfigurasi yang cukup dan metode verifikasi yang akan digunakan selama proses instalasi EDR Cybereason.

1.2 Analisa Resiko

Dalam melakukan instalasi EDR Cybereason tidak terdapat downtime dan disarankan agar semua kegiatan ini dilakukan pada jadwal yang sudah ditentukan, disetujui, dan dipahami oleh Tenant PDNS. Selama waktu kegiatan diharapkan tidak ada perubahan network atau konfigurasi diluar aktivitas yang direncanakan tanpa terlebih dahulu diverifikasi oleh tim Telkomsigma dan tim Tenant PDNS.

2 Ringkasan

2.1 Ringkasan Aktivitas

Nama Aktivitas	Instalasi EDR Cybereason
Alasan	Instalasi EDR Cybereason untuk Tenant PDNS
Jenis Pengerjaan	Instalasi
Waktu Pelaksanaan	TBD
Layanan Terdampak	Tidak Ada
Lama Dampak Layanan	Tidak Ada
Prasyarat	Membuka Policy Rules Pada Firewall untuk komunikasi dari sensor EDR ke Server Cybereason SAAS dan sebaliknya.

Table 2-1 Ringkasan Aktivitas

2.2 Strategi Pengerjaan

Pengerjaan Instalasi perangkat memerlukan adanya perhatian terhadap proses konfigurasi dan kesiapan koneksi. Namun perlu adanya strategi untuk mengurangi resiko kesalahan pengerjaan yang tidak diinginkan agar tercapai keberhasilan dalam proses Instalasi.

Berikut adalah langkah-langkah aktivitas yang akan dilakukan dalam pengerjaan kali ini :

- Activity 1 Persiapan
- Activity 2 Instalasi
- Activity 3 Rollback

Berikut jadwal dan pengerjaan yang dapat dilakukan pada tabel dibawah ini.

2.3 Langkah-langkah Kegiatan

Ringkasan Tugas	Pelaksana	Waktu pengerjaan
Persiapan :		
Persiapan Instalasi EDR Cybereason	Sigma & Tenant	35 Menit
Instalasi :		
Instalasi EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux	Sigma & Tenant	40 Menit
Instalasi EDR Cybereason Pada Sistem Operasi Ubuntu/Debian	Sigma & Tenant	40 Menit
Instalasi EDR Cybereason Pada Sistem Operasi Windows	Sigma & Tenant	15 Menit
Rollback :		
Uninstall EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux	Sigma & Tenant	15 Menit
Uninstall EDR Cybereason Pada Sistem Operasi Ubuntu/Debian	Sigma & Tenant	15 Menit
Uninstall EDR Cybereason Pada Sistem Operasi Windows	Sigma & Tenant	15 Menit
TOTAL Durasi		175 Menit

Table 2-2 Langkah-langkah Kegiatan

2.4 Dampak Aktivitas

Tidak Ada.

2.5 Aktivitas Downtime

Tidak Ada.

2.6 Waktu Pelaksanaan

Aktifitas	Deskripsi	Waktu
Persiapan	Persiapan Pre-check requirement & service	TBD
Mulai Aktifitas	Mulai aktifitas pada jadwal yang telah disepakati	TBD
Selesai Aktifitas	Akhir dari aktivitas	TBD

Table 2-5 Waktu Pelaksanaan

3 Topologi

3.1 Logical Topology

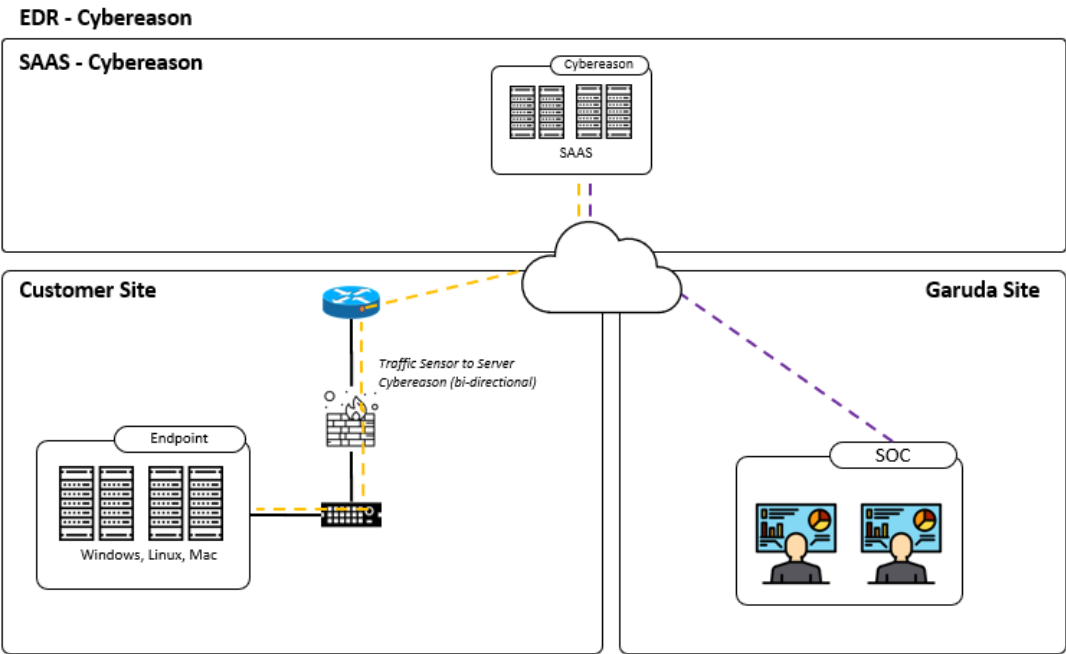


Table 3-1 Logical Topology

4 Persiapan

4.1 Persiapan Instalasi EDR Cybereason

Nama Kegiatan	Persiapan Instalasi EDR Cybereason
Waktu Pelaksanaan	TBD
Lama Pengerjaan	35 Menit
Layanan Terdampak	Tidak Ada
Tujuan	Melakukan Persiapan Instalasi EDR Cybereason
Analisa Terdampak	Tidak Ada
Perangkat Terkait	TBD

No	Durasi	Pekerjaan	Detail Pengerjaan	Perangkat	PIC	Downtime	Status
1	15 Menit	Download Installer Cybereason & Precheck Scripts Linux	Melakukan download installer Cybereason & Precheck Scripts Linux pada URL : https://tinyurl.com/yck5c3ht	TBD	Sigma	No	☐ Pass ☐ Fail ☐ N/A
2	15 Menit	Membuka Policy Rules Pada Firewall	Membuka Firewall Rules untuk komunikasi dari sensor EDR ke Server Cybereason SAAS dan sebaliknya. - Traffic inbound & outbound IP Address (34.146.121.252, 34.84.38.129, 35.221.72.65) dengan port 80, 443, 8443 (IP Region Jepang). - Traffic inbound & outbound (FQDN *.cybereason.net) dengan port 80, 443, 8443.	TBD	SecOPS PDNS	No	☐ Pass ☐ Fail ☐ N/A
3	5 Menit	Melakukan Pengecekan Versi Sistem Operasi	SUPPORTED OS VERSIONS FOR THE SENSOR : Versi sistem operasi yang disupport untuk sensor : - Windows 11, up to Windows 11 23H2 - Windows 10, up to Windows 10 22H2 - Windows 10 IoT - Windows 8.1 - Windows 8 - Windows Server 2022 - Windows Server 2019 - Windows Server 2016 - Windows Server 2012 R2 - Windows Server 2012	TBD	Sigma	No	☐ Pass ☐ Fail ☐ N/A

			11. Windows Server 2008 R2 SP1 12. CentOS 7, 8 13. Red Hat Enterprise Linux 7, 8, 9 14. Oracle Linux 7, 8, 9 15. Ubuntu 14 LTS, 16 LTS, 18.04 LTS, 20.04 LTS, 20.10, 22.04 LTS, 22.10, 23.04 16. SLES 12 (limited support), 15 17. Debian 8, 9, 10, 11, 12 18. Amazon Linux AMI 2017.03, Amazon Linux 2, Amazon Linux 2023 19. Rocky Linux 8.5, 8.6, 9.x 20. CloudLinux 7 21. AlmaLinux 8.6, 9.x Note : • For Windows : Cybereason platform supports both the 32-bit and 64-bit versions. • For Linux : Cybereason sensors do not support 32-bit operating systems.				
--	--	--	--	--	--	--	--

Table 4-1 Persiapan Instalasi EDR Cybereason

5 Instalasi

5.1 Instalasi EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux

Nama Kegiatan	Instalasi,EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux
Waktu Pelaksanaan	TBD
Lama Pengerjaan	40 Menit
Layanan Terdampak	Tidak Ada
Tujuan	Melakukan Instalasi,EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux
Analisa Terdampak	Tidak Ada
Perangkat Terkait	TBD

No	Durasi	Pekerjaan	Detail Pengerjaan	Perangkat	PIC	Downtime	Status
1	5 Menit	Pengecekan Versi Sistem Operasi	Melakukan pengecekan versi sistem operasi pada vm yang akan diinstall sensor EDR	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
2	5 Menit	Izin Menggunakan Script	Memberikan izin atau permission untuk menggunakan script chmod +x install_dependencies.sh	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
3	5 Menit	Precheck Scripts Linux	Menjalankan precheck scripts linux untuk mengetahui packages yang telah diinstall. ./install_dependencies.sh -t dependencies.txt	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
4	15 Menit	Install Required Packages	Melakukan install packages jika ada packages yang belum diinstall.	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
5	10 Menit	Install Cybereason Sensor	Melakukan install Cybereason sensor sudo rpm -ivh <RPM file>	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
6	10 Menit	Check Service Cybereason	Melakukan check service Cybereason berjalan atau tidak systemctl status cybereason-sensor	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A

Table 5-1 Instalasi EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux

5.2 Instalasi EDR Cybereason Pada Sistem Operasi Ubuntu/Debian

Nama Kegiatan	Instalasi,EDR Cybereason Pada Sistem Operasi Ubuntu/Debian
Waktu Pelaksanaan	TBD
Lama Pengerjaan	40 Menit
Layanan Terdampak	Tidak Ada
Tujuan	Melakukan Instalasi,EDR Cybereason Pada Sistem Operasi Ubuntu/Debian
Analisa Terdampak	Tidak Ada
Perangkat Terkait	TBD

No	Durasi	Pekerjaan	Detail Pengerjaan	Perangkat	PIC	Downtime	Status
1	5 Menit	Pengecekan Versi Sistem Operasi	Melakukan pengecekan versi sistem operasi pada vm yang akan diinstall sensor EDR	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
2	5 Menit	Izin Menggunakan Script	Memberikan izin atau permission untuk menggunakan script chmod +x install_dependencies.sh	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
3	5 Menit	Precheck Scripts Linux	Menjalankan precheck scripts linux untuk mengetahui packages yang telah diinstall. ./install_dependencies.sh -t dependencies.txt	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
4	15 Menit	Install Required Packages	Melakukan install packages jika ada packages yang belum diinstall.	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
5	10 Menit	Install Cybereason Sensor	Melakukan install Cybereason sensor sudo dpkg -i <deb files>	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
6	10 Menit	Check Service Cybereason	Melakukan check service Cybereason berjalan atau tidak systemctl status cybereason-sensor	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A

Table 5-2 Instalasi EDR Cybereason Pada Sistem Operasi Ubuntu/Debian

5.3 Instalasi EDR Cybereason Pada Sistem Operasi Windows

Nama Kegiatan	Instalasi,EDR Cybereason Pada Sistem Operasi Windows
Waktu Pelaksanaan	TBD
Lama Pengerjaan	15 Menit
Layanan Terdampak	Tidak Ada
Tujuan	Melakukan Instalasi,EDR Cybereason Pada Sistem Operasi Windows
Analisa Terdampak	Tidak Ada
Perangkat Terkait	TBD

No	Durasi	Pekerjaan	Detail Pengerjaan	Perangkat	PIC	Downtime	Status
1	5 Menit	Pengecekan Versi Sistem Operasi	Melakukan pengecekan versi sistem operasi pada vm yang akan diinstall sensor EDR	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
2	10 Menit	Install Cybereason Sensor	Melakukan install Cybereason sensor 1. Execute file installer sesuai versi sistem operasi 2. Akan muncul menu Cybereason Setup Wizard lalu click install 3. Lalu proses instalasi akan berjalan 4. Instalasi sukses ditandai dengan notif "Installastion Completed Successfully"	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A

Table 5-3 Instalasi EDR Cybereason Pada Sistem Operasi Windows

6 Rollback

6.1 Uninstall EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux

Nama Kegiatan	Uninstall EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux
Waktu Pelaksanaan	TBD
Lama Pengerjaan	15 Menit
Layanan Terdampak	Tidak Ada
Tujuan	Melakukan Uninstall EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux
Analisa Terdampak	Tidak Ada
Perangkat Terkait	TBD

No	Durasi	Pekerjaan	Detail Pengerjaan	Perangkat	PIC	Downtime	Status
1	5 Menit	Stop Service Cybereason	Melakukan stop service Cybereason. sudo systemctl stop cybereason-sensor	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
2	10 Menit	Uninstall EDR Cybereason	Melakukan uninstall EDR Cybereason sudo rpm -e cybereason-sensor	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A

Table 6-1 Uninstall EDR Cybereason Pada Sistem Operasi Centos/RHEL/Oracle Linux/Amazon Linux

6.2 Uninstall EDR Cybereason Pada Sistem Operasi Ubuntu/Debian

Nama Kegiatan	Uninstall EDR Cybereason Pada Sistem Operasi Ubuntu/Debian
Waktu Pelaksanaan	TBD
Lama Pengerjaan	15 Menit
Layanan Terdampak	Tidak Ada
Tujuan	Melakukan Uninstall EDR Cybereason Pada Sistem Operasi Ubuntu/Debian
Analisa Terdampak	Tidak Ada
Perangkat Terkait	TBD

No	Durasi	Pekerjaan	Detail Pengerjaan	Perangkat	PIC	Downtime	Status
1	5 Menit	Stop Service Cybereason	Melakukan stop service Cybereason. sudo systemctl stop cybereason-sensor	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A
2	10 Menit	Uninstall EDR Cybereason	Melakukan uninstall EDR Cybereason sudo dpkg -r cybereason-sensor	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A

Table 6-2 Uninstall EDR Cybereason Pada Sistem Operasi Ubuntu/Debian

6.3 Uninstall EDR Cybereason Pada Sistem Operasi Windows

Nama Kegiatan	Uninstall EDR Cybereason Pada Sistem Operasi Windows
Waktu Pelaksanaan	TBD
Lama Pengerjaan	15 Menit
Layanan Terdampak	Tidak Ada
Tujuan	Melakukan Uninstall EDR Cybereason Pada Sistem Operasi Windows
Analisa Terdampak	Tidak Ada
Perangkat Terkait	TBD

No	Durasi	Pekerjaan	Detail Pengerjaan	Perangkat	PIC	Downtime	Status
2	15 Menit	Uninstall EDR Cybereason	Melakukan uninstall EDR Cybereason Uninstall EDR Cybereason pada control panel → program and features	TBD	Sigma & Tenant	No	☐ Pass ☐ Fail ☐ N/A

Table 6-3 Uninstall EDR Cybereason Pada Sistem Operasi Ubuntu/Debian

7 Persetujuan Method of Procedure

Nama Proyek : EDR Cybereason
Deskripsi Sistem : EDR
Document Version : 1.0

Method Operation Procedure ini menjelaskan langkah-langkah yang dibutuhkan untuk Pekerjaan EDR Cybereason untuk Tenant PDNS dan sudah disetujui oleh Telkomsigma dan Tenant PDNS.

Sign Off			
<u>Nama :</u>	<u>Nama :</u>	<u>Nama :</u>	<u>Nama :</u>
<u>Perusahaan :</u>	<u>Perusahaan :</u>	<u>Perusahaan :</u>	<u>Perusahaan :</u>
<u>Jabatan :</u>	<u>Jabatan :</u>	<u>Jabatan :</u>	<u>Jabatan :</u>

Catatan:
