FreeDivision/ReaQta Data Processing

verze 1.1

4. června 2021

OBSAH

FreeDivision/ReaQta Privacy Policy

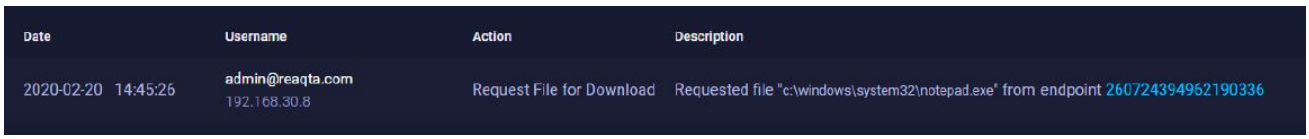
ReaQta je zpracovatelem osobních údajů společnosti **FreeDivision s.r.o.** se sídlem, Ďáblická 136/51, Ďáblice, 182 00 Praha 8 a pobočkou Rektorská 50/52, Malešice, 108 00 Praha 10, IČO: 27367789, DIČ: CZ27367789; zapsané v OR vedeném u Městského soudu v Praze v oddílu C, vložce č. 108828 (dále jen „**zpracovatel**“) a jakožto zpracovatel jedná dle pokynů správce, tj. společnosti FreeDivision s.r.o. na základě smlouvy o zpracování osobních údajů uzavřené dle čl. 28 GDPR. ReaQta jakožto zpracovatel taktéž jedná v souladu s evropským obecným nařízením o ochraně osobních údajů (tj. nařízením EU č. 2016/679, dále jen „obecné nařízení o ochraně údajů“ - GDPR), jakož i národními právními předpisy, mimo jiné zákonem č. 110/2019 Sb., o zpracování osobních údajů, v platném znění, za účelem ochrany osobních údajů partnerů i zákazníků (fyzických osob) a s tím souvisejícího zmírnění rizika nežádoucího úniku osobních a/nebo citlivých informací. Tento dokument přitom navazuje na Privacy Policy společnosti **FreeDivision s.r.o.** dostupné na Zásady zpracování OU_FD_final3.docx (freedivision.com) a blíže Vás informuje o způsobech zpracování osobních údajů ze strany společnosti FreeDivision/ReaQta ohledně konkrétních produktů, které nabízíme jako je FreeDivision Cloud.

On Premise nasazení

ReaQta-Hive podporuje nasazení On Premise, kde je server (Hive-Brain) nasazen v datovém centru zákazníka. Data (ve formě metadat), která se přenášejí z koncových bodů na server, zůstávají v samotném datovém centru.

Zákazník nebo partner, který vlastní infrastrukturu, má nad daty úplnou kontrolu. ReaQta může čas od času a se svolením zúčastněných stran přistupovat k těmto údajům za účelem poskytování běžné nebo mimořádné údržby a podpůrných služeb.

Z koncových bodů se do Hive-Brain vždy přenášejí pouze metadata. Další a konkrétní datové přenosy mohou iniciovat operátoři dashboardu. Takové akce jsou vždy protokolovány na stránce auditu a nelze je změnit bez zásahu do Hive-Brain:



Ve výchozím nastavení je **uchování dat 30 dní**, ale tento limit lze prodloužit nebo snížit podle preferencí zákazníka nebo partnera.

Další komponenty (Hive-Cloud a Hive-Cloud Enrichment)

Nasazení On Premis mohou zahrnovat další komponenty Opt-In.

- Hive-Cloud
- Hive-Cloud Enrichment

Oba komponenty fungují výhradně na metadatech (hashe souborů a IP adresa), tyto informace se přenášejí do ReaQty, aby se obohatily výstrahy a poskytly další úrovně ochrany. Taková metadata mohou být používána ReaQtou, během procesu obohacování, k dotazování na externí databáze, například k poskytnutí dalších informací o hrozbách, reputaci IP atd.

Cloudové nasazení

Za Cloudové nasazení ReaQty se považuje, pokud je Hive-Brain hostován a udržován ReaQtou/FreeDivision. Cloudová nasazení přenášejí telemetrii a forenzní data z koncových bodů do Hive-Brain ovládaného ReaQtou.

Z koncových bodů se do Hive-Brain vždy přenášejí pouze metadata. Další a konkrétní datové přenosy mohou iniciovat operátoři dashbordu. Takové akce se vždy zaznamenávají na stránce auditu a nelze je změnit bez zásahu do Hive-Brain.

Uživatelé dashboardu mohou požadovat:

- Specifické soubory koncových bodů
- Forensics Kit obsahující forenzní důkazy získané přímo z koncového bodu a přenesené na server s uchováváním dat 1 den.

Obecná metadata (telemetrie):

- Interní IP adresu
- Hostname koncového bodu
- Detail operačního systému (OS Verse, CPU detail, seznam instalovaných aplikací)
- Seznam Mac adres
- Doménovou adresu, pokud koncový bod využívá doménu

Obsahuje události doménového řadiče:

- Časové razítko události
- Úplná cesta procesu
- Koncový bod / uživatelské jméno
- Zpracovat úroveň oprávnění
- Cesta k souboru s příslušnou operací se souborem
- Procesní a / nebo hašovací soubor (MD5, SHA-1, SHA-256)
- Operace se soubory (čtení / zápis / mazání)
- Činnosti registru (cesta k registru, klíč, hodnota)
- Síťová aktivita (IP adresa, protokol, směr odchozí / příchozí)
- Informace o aktivitě účtu (název účtu, předmět a cílová adresa, metadata se mohou lišit podle typu aktivity účtu)

Výchozí **uchování dat** je **30 dní**.

Seznam událostí

Událost je kolekce metadatových informací přenesených z koncového bodu do Hive-Brain. Níže je uveden seznam shromážděných událostí.

ProcessCreated
ProcessTerminated
ProcessInjected
FileCreated
FileRenamed
FileDeleted
NetworkConnectionEstablished
RegistryPersistence
RegistryValueSet
RegistryEntryDeleted
FileWritten
ExecutableDropped
ExecutableDuplicatedSelf
Keylogging
Screenshot
PrivilegeEscalation
FileSystemPersistence
ProcessImpersonated
FileRead
SignatureForged
CredentialHarvested
WhitelistTriggered
Dll-Sideloaded
SuspiciousScriptExecuted
BlacklistTriggered
EndpointStartedUp
IncidentTerminated
AnomalousBehaviour
TokenStolen
ProtectionPolicyTriggered
RansomwareBehaviour
RemoteAccessToolBehaviour
WmiActivity11
WinINetActivity
WinDnsClientActivity
AccountLoggedOn
AccountLogonFailed
AccountCredentialsValidationAttempted
ExplicitCredentialsLogonAttempted
AndroidMicrophoneOn
AndroidMicrophoneOff
AndroidCameraOn
AndroidCameraOff
Android PackageInstalled
AndroidPackageRemoved
DetectionTriggered
RemediationProcessKilled
RemediationEndpointIsolated
RemediationFileDeleted
KerberosAuthTicketRequested
KerberosServiceTicketRequested
KerberosPreAuthFailed
LogonSpecialPrivAssigned
ModuleLoaded
WmiProcessCreated
MacroEnabledDocument
InMemoryExecutable
ProcessKilled
AdversarialTechniqueDetected
Mitre Att&ck
WmiEventFilter
WmiEventConsumer
WmiFilterToConsumer
RegistryKeyCreated
ComHijacked
UserAccountCreated (4720)
UserAccountDeleted (4726)
RemediationRegistryValueDeleted
PowershellScriptBlockLogged
EtwSecurityAuditing
AntivirusDetectionNP
AntivirusDetection
RemediationAntivirus
RemediationQuarantinedFileDeleted
RemediationQuarantinedFileRestored
ScheduledTaskCreated
ScheduledTaskDeleted
ScheduledTaskUpdated
ScheduledTaskExecuted
ServiceCreated
ServiceDeleted
ServiceStarted
ServiceStopped
AMSI
AdversarialTechniqueDetectedNP

Hive-Cloud and Hive-Cloud Enrichment

Hive-Cloud a Hive-Cloud Enrichment jsou Opt-In a lze je kdykoli vypnout.

Oba komponenty fungují výhradně na metadatech (hashe souborů a IP adresa), tyto informace se přenášejí do ReaQta, aby se obohatily výstrahy a poskytly další úrovně ochrany. Taková metadata mohou být používána ReaQtou během procesu obohacování k dotazování na externí databáze, například k poskytnutí dalších informací o hrozbách, reputace IP atd.

Údržba a odstraňování problémů

Během běžné a mimořádné údržby, jako jsou aktualizace, upgrady nebo odstraňování problémů, může ReaQta/FreeeDivision vyžadovat dočasný přístup k datům koncových uživatelů, která mohou obsahovat osobně identifikovatelná data, jako například:

- IP adresy
- Uživatelská jména
- Názvy počítačů
- Obecná metadata (názvy souborů, velikost souboru, doba vytvoření, doba odstranění atd.)

Taková data společnost ReaQta/FreeDivision neshromažďuje ani nezpracovává nad rámec činností odstraňování problémů.