

ReaQta Hive

I. Přehled funkcionalit a popis jednotlivých modulů

a. Pokročilá detekce na základě chování procesů

- Detekční jádro ReaQta-Hive dokáže spolehlivě odhalit útoky na infrastrukturu pomocí chování jednotlivých procesů.
- Umožňuje zobrazit a rekonstruovat tzv. storyline útoku, pokud se nachází v módu Hunting (lov).
- Automaticky hodnotí jednotlivé operace procesů a celkově událost hodnotou vážnosti problému (od 0 do 100) dle závažnosti operací.
- Dokáže přehledně zopsat provedené operace jednotlivých procesů (včetně detailů, například obsah HTTP komunikace) v rámci události, kterou jádro Hive označí sám, nebo ji označí manuálně uživatel na základě logů z koncových zařízení.

b. Kompletní auditní záznamy

- ReaQta ve výchozím nastavení zaznamenává jakékoliv akce administrátorů a uživatelů v cloud rozhraní ReaQta Hive bez smazání po určitém čase, vč. nezdařených pokusů o přihlášení do cloud rozhraní.
- ReaQta ukládá logy koncových zařízení s výchozí datovou retencí 30 dnů.
 - V případě, že se určité logy týkají události, jsou uchovány bez smazání po určitém čase.
- Možnost exportu vyfiltrované části záznamů do souboru .csv

c. Správa inventáře (koncových zařízení)

- Automatická identifikace a možnost štítkování koncových zařízení, na kterých byl a stále nainstalován agent ReaQta pro koncové stanice.
- Uchovává informace o aktuálním operačním systému; aktuální verzi agenta ReaQta; architekturu; typ procesoru; MAC adresy všech síťových rozhraní; IP adresu, přes kterou komunikuje koncové zařízení s ReaQta Hive serverem.
- Možnost štítkovat koncová zařízení jako virtuální stroje anebo servery.
- Sleduje stav koncového zařízení (zda-li je online) a zobrazuje graf za posledních 24 hodin.
- Možnost štítkování zařízení a přidávání do skupin.
- Možnost odinstalovat na dálku agenta ReaQta v konzoli.
- Možnost izolovat koncové zařízení od internetu (zakáže všechna síťová spojení kromě komunikace s ReaQta konzolí).
- V detailu koncového zařízení je možné zobrazit si seznam akcí provedených na koncovém zařízení – každý z těchto logů lze využít k manuálnímu vytvoření události.
- Možnost pracovat s online zjednodušenou konzolí zařízení:
 - Zobrazit aktuální procesy (Windows, Linux, macOS)
 - Možnost proces vypnout, pozastavit, stáhnout soubor nebo si zobrazit moduly vybraného procesu.
 - Je zde možnost vyhledávat dle PID, PPID, názvu procesu nebo spouštějícího uživatele.

- Zobrazit služby (Windows)
 - Možnost vyhledávat dle typu nebo názvu služby.
- Zobrazit aktuální síťová spojení (Windows)
 - Možnost vyhledávat dle PID, cesty k souboru, lokální adresy a vzdálené adresy. Zobrazuje i porty připojení
- Stažení souboru z definované cesty (Windows, Linux, macOS)
- Smazání souboru z definované cesty (Windows, Linux, macOS)
- Zobrazit moduly načtené procesem dle definovaného PID (Windows)
- Získat nainstalované aplikace na telefonu (Android)
- Stažení aplikace z telefonu (Android)

d. Možnost tvorby vlastních reportů

- Umožňuje generovat reporty za vybraný časový interval a exportovat je do souboru PDF.
- Možnost nastavit pravidelné generování na jednotlivé dny v týdnu či ad-hoc generování.
- Obsahem reportu je:
 - krátký výpis událostí vč. grafů,
 - počet událostí,
 - reakční doba v uzavírání událostí,
 - grafický poměr aktivní vs. vyřešené události,
 - grafický přehled rozdělení událostí dle závažnosti,
 - grafický přehled nejběžnějších typů událostí,
 - detaily jednotlivých událostí seřazených dle závažnosti,
 - report infrastruktury:
 - počet fyzických stanic,
 - počet virtuálních strojů,
 - počet nově zaregistrovaných koncových zařízení,
 - počet neaktivních koncových zařízení,
 - grafický přehled všech typů (a verzí) operačních systémů.
 - Možnost přidat své textové komentáře do výsledného reportu:
 - textový souhrn pro vedení (Executive Summary),
 - textový souhrn týkající se bezpečnosti (Security Summary),
 - textový souhrn týkající se událostí (Alerts Report Summary),
 - textový souhrn týkající se infrastruktury (Infrastructure Report Summary).
- Možnost nastavit si emailová upozornění na nově vygenerovaný report.

e. Automatizovaná aktivní ochrana koncových bodů

- Automatická ochrana před nebezpečnými aktivitami na koncových stanicích jako například ransomware, zranitelnosti jádra OS, anomálie v běžném chování zařízení.
- Možnost vytvářet pravidla – whitelist/blacklist dle různých typů událostí.
 - Možnost zobrazit priority mezi zvolenými pravidly pro snadné řešení problémů s prioritami.
 - Pravidla jsou rozdělena dle potřebného rozsahu. Je zde možnost vytvářet tzv. globální nebo skupinová pravidla.
 - Každý typ událostí umožňuje blíže specifikovat rozsah blokování (např. na celou složku, samotnou aplikaci, hash dané aplikace nebo chování procesu).
- Obsahuje základní seznam ochranných pravidel (Protection pravidla) chránící:

- Operace mezi procesy (Cross-process Operation)
- Chování ransomwarů (Ransomware Behavior)
- Eskalace oprávnění (Privilege Escalation)
- Získávání tokenů (Token Stealing)
- Podvržení podpisů aplikací (Forged Digital Signature)
- Napodobení procesu (Process Impersonation)
- Podezřelé skripty (Suspicious Script)
- Anomální chování (Anomalous Behavior)
- Podvržení DLL knihoven (DLL Hijacking)
- Pasivní ochrana dat vůči zašifrování ransomware (nezávislé na typu ransomware).
 - Data jsou agentem před zašifrováním zálohována do stejné složky, jen s jinou příponou.
- Možnost štítkování události a přidávání do skupin.
- Možnost zapsat interní poznámky k dané události.
- Možnost manuálně upravit hodnotu závažnosti události

f. Online analýza souborů virovými databázemi

- Analýza souborů online databází VirusTotal a AlienVault.
 - Opětovná analýza souborů lze zpětně vyžádat v konzoli uživatelem.
- Analýza probíhá na základě metadat.
- Slouží převážně pro rychlou možnost ověřit závažnost vyvolané události a snadněji identifikovat a oddělit potenciálně škodlivé soubory od neškodných dat.
- Na vyžádání je možnost povolit modul, který automaticky při nálezů škodlivého souboru vytvoří blokující/upozorňovací pravidlo přímo na tento daný typ souboru. Takové pravidlo je poté platné na celou infrastrukturu.

g. Pokročilá forenzní analýza

- Modul forenzní analýzy umožňuje zobrazit uživateli více podrobnosti k jednotlivé události, nebo samotné operaci v logu. Z těchto samotných operací z logu dokáže uživatel snadno vytvořit událost manuálně, díky čemuž ReaQta bude následně stejné události po několika označení jako škodlivé sama vyvolávat (strojové učení).
- Takto vytvořené události jsou plnohodnotné a jsou uloženy navždy v ReaQta.
- Umožňuje vidět detaily jednotlivých procesů, metadata spustitelných souborů, počet podobných událostí v rámci infrastruktury.
- Pokud je koncové zařízení online, lze z něj stáhnout i soubory související s událostí – tyto soubory se stáhnou do počítače nebo je možnost si je prohlédnout přímo v konzoli ReaQta (náhled má omezení souborů do 50 MB). Stažený soubor je v ReaQta konzoli uchován po dobu 24 hodin, poté je potřeba soubor stáhnout z koncového zařízení znovu (za předpokladu, že se na zařízení stále nachází).
- U každé vygenerované události je vytvořený i tzv. behaviorální strom, který umožňuje rychlý grafický náhled na celý postup útoku dle procesů a umožňuje zobrazit nejdůležitější informace o procesech vč. možnosti lovu procesu, stažení spustitelného souboru nebo vytvoření blokujícího pravidla.
 - Strom je možný vyexportovat ve svém rozložení do obrázku .png
 - Ve stromu jsou zobrazeny i jednotlivé MITRE techniky vč. detailu techniky.

h. Analýza souvisejících souborů (artefaktů)

- Detekce a analýza rozšíření souborů souvisejících s událostí napříč celou infrastrukturou v detailu události.
- Veškeré soubory, které byly vytvořeny procesy souvisejícími s událostmi jsou evidovány a graficky zobrazeny v detailu události.
- Každý tento artefakt je porovnán vůči celé infrastruktuře, díky kterému je snadné zjistit, zda je soubor na koncových stanicích běžný či nakolik je potenciálně škodlivý soubor rozšířen do infrastruktury.

i. Možnost tvorby vyšetřovacích balíčků

- V rámci koncových stanic je možné vygenerovat zaheslovaný archiv formátu .zip.
- Tyto balíčky jsou dostupné 24 hodin od vygenerování.
- Je možnost výběru rozsáhlosti souborů:
 - Základní balík (tvorba probíhá kolem 5 minut)
 - Spuštěné procesy (.csv)
 - Služby (.csv)
 - Aktivní síťová spojení (.txt)
 - ARP mezipaměť (.txt)
 - DNS mezipaměť (.txt)
 - Informace o systému (.csv)
 - Nainstalované programy (.csv)
 - Aktualizace (.csv)
 - Bezpečnostní záznamy událostí (Event logs - security) (.evtx)
 - Naplánované akce (.csv)
 - Uživatelé a skupiny (.csv)
 - Sdílené disky (.csv)
 - Informace o proxy (.txt)
 - Časové pásmo (.csv)
 - Síťová konfigurace (.txt)
 - Pokročilý balík (tvorba probíhá kolem 15 minut)
 - Základní balík
 - Chybějící aktualizace (.csv)
 - Proměnné prostředí (.csv)
 - Přednačtené soubory (Prefetch) (.csv)
 - Informace k BitLocker (.txt)
 - Pojmenované „pipes“ (.txt)
 - SMB relace (protokol Samba) (.txt)
 - Asociace přípon souborů (.xml)
 - Soubor „hosts“
 - Rozšířený export záznamů událostí (.evtx)
 - Aktuální nastavení UAC (.txt)
 - Auditní politiky (.txt)
 - Pravidla firewallu (.csv)

j. Automatizované ošetření zařízení po útoku

- Tzv. remediace umožňuje přes grafické rozhraní následující kroky:
 - Ukončit procesy
 - Odstranit soubory vytvořené malwarem

- Odstranit perzistenční nastavení (uložené na disku a v registrech)
- Izolovat koncové zařízení
- ReaQta umožňuje remediaci přímo k události s tím, že zvýrazní akce, které její jádro doporučuje provést.

k. Lov hrozeb

- Pokročilý nástroj pro hledání aktivit v záznamech získaných z koncových zařízení.
- Zobrazuje záznamy v reálném čase a historii až 30 dní zpět (pokud záznam byl v rámci události, tak je uložen bez odstranění)
- Umožňuje hledat záznamy dle klienta (v případě multi-tenant verze), skupin, koncových zařízení a typu aktivit.
 - Zároveň poskytuje možnosti hledání dle určitých parametrů, které se objevují v záznamech.
 - Umožňuje hledat dle indikátorů kompromitace (IoC), specifického chování nebo indikátorů a detailu procesů.

l. Detekční strategie DeStra

- Nástroj pro tvorbu pokročilých automatizačních pravidel.
- Vhodný pro vytváření vlastních detekcí, automatického chování vůči specifickým hrozbám a tvorbu vlastních ošetřovacích procesů.
- Veškeré DeStra strategie se píšou ve skriptovacím jazyce Lua a YARA.

m. Mitre ATT&CK™

- Automatizované řazení chování hrozeb k Mitre taktikám a technikám, které se využívají ke kategorizaci útoků dle jednotlivých úrovní tzv. kill-chain.
- ReaQta zobrazuje přehledný panel, kde jsou vidět grafy počtu použitých technik v rámci infrastruktury v daném období. Po rozkliknutí jednotlivé techniky útoku je možné přejít na vyhledávání v panelu Lovu hrozeb, díky čemuž je snadné vyhledat veškeré aktivity v infrastruktuře, které využívají tyto techniky.
- Všechny taktiky a techniky útoků jsou podrobně popsány v anglickém jazyce.

n. API přístup ke konzoli

- Přímé napojení na API ReaQta konzole, užiteční pro automatizaci určitých pracovních procesů na míru danému klientovi.
- Umožňuje integraci s externími platformami, například SIEM.

o. Správa uživatelů ReaQta

- ReaQta konzole umožňuje vytvářet uživatelské účty s různými typy oprávnění k datům a akcím.
- ReaQta umožňuje vytvořit uživatele s oprávněním Administrátora (Administrator), Respondenta (Responder), Analytika (Analyst) a Sledujícího (Observer)
 - V případě multi-tenant verze, ReaQta umožňuje vytvořit uživatele navíc s možností definovat pole působnosti uživatele – buďto tzv. globálního uživatele, nebo uživatele tennanta.
- Administrátor má plná oprávnění, umožňuje upravovat veškerá koncová zařízení, tvořit nové uživatele a skupiny.
- Respondent má oprávnění k nahlížení a modifikaci koncových zařízení, remediaci a tvorbě pravidel.

- Analytik má oprávnění pouze nahlížet na hlavní obrazovku a spravovat příchozí události, nemá oprávnění k úpravě politik a k provedení jakýchkoliv operací s koncovými zařízeními.
- Sledující jsou pouze uživatelé, kteří nemají přístup k jakýmkoliv operacím, slouží pouze jako uživatelé pouze pro čtení.
- Administrátor může vynutit 2FA ověřování (pomocí OTP aplikace jako např. Google Authenticator)
- V detailu uživatele jsou zobrazeny veškerá zařízení, která jsou při přihlášení uživatele vybrána jako důvěryhodná zařízení – zároveň je možné z těchto zařízení uživatele odhlásit.

p. Notifikace na události a akce v konzoli

- Notifikace uživatelů probíhá v reálném čase na panelu notifikací v konzoli ReaQta, nebo přes email uživatele.
- Administrátor může upravovat, jaké typy notifikací mají využívat notifikace v konzoli, nebo emailové upozornění.
- U upozornění přes email je třeba nastavit administrátorem SMTP údaje.

q. Správa verzí agentů

- Modul umožňuje spravovat jednotlivé verze agentů ReaQta a nahrávat je do konzole pro další využití.
- Možnost povolení a zakázání jednotlivých verzí agentů.
- Při stažení možnost vygenerovat identifikátory skupiny/tenanta.

r. Správa tenantů (v případě multi-tenant verze)

- Možnost vytvářet jednotlivé tenanty (společnosti) v rámci jedné multi-tenant licence, kde je možnost přerozdělovat zakoupené licence mezi jednotlivé tenanty a nastavovat licencím platnost až do doby platnosti hl. licence.
- U tenanta je možnost definovat logo, název a interní popis.
- V rámci tenanta je možnost vytvářet jednotlivé skupiny a podskupiny.
- Globální uživatel může monitorovat všechny tenanty najednou, nebo si může přepínat zobrazení.

s. NanoOS

- Součást agenta pro platformy Windows.
- Jedná se o SW řešení, které operuje mimo součásti operačního systému, zaznamenává a vyhodnocuje jednotlivé události. Pracuje na úrovni privilegovaného režimu -1 (tedy ještě před jádrem OS – úroveň 0).
- Díky své pozici před jádrem OS je NanoOS ochráněno před veškerým malwarem.
- Jedná se o součást ReaQta agenta, která vyžaduje virtualizaci (funguje jako komponenta hypervizoru) – musí ji podporovat CPU a v BIOS musí být povolena.
- Funguje nezávisle na spuštěných procesech, do kterých nedělá žádné úpravy.

II. Požadavky na koncová zařízení

a. Specifikační tabulka

Operační systém	Verze	Místo na disku	Využití paměti	Požadavky na síťové připojení
Windows Client *	7 (SP1), 8, 8.1, 10, 10-POS (plně aktualizovaná)	90MB	Přibližně 60MB	10Mb+
Windows Server *	2008R2(SP2), 2012, 2016, 2019 (plně aktualizovaná)	90MB	Přibližně 60MB	10Mb+
Linux	Ubuntu (16 / 18), Centos 7, Debian 8.10, RedHat 7, Mint 18+	90MB	Přibližně 60MB	10Mb+
MacOS	Sierra+	90MB	Přibližně 60MB	10Mb+
Android	4.2+	90MB	Přibližně 60MB	10Mb+

** Pro úplnou ochranu ReaQtou pomocí NanoOS musí koncové zařízení podporovat virtualizaci VT-x (Intel) nebo AMD-V (AMD), která musí být zapnuta v BIOS. Pokud je na koncovém zařízení využívána virtualizace jiným procesem, NanoOS je automaticky vypnut, aby nekolidoval s aplikacemi, které virtualizaci využívají.*