Non-stop sigurnosna za

Rješenje IBM QRadar on Cloud mrežna je inteligencija i analitička usluga koja otkriva napade na informacijsku infrastrukturu vaše tvrtke

Zvonko Pavić

Rješenje IBM QRadar SIEM (Security Information and Event Management) rješenje je za sigurnosnu zaštitu svih segmenata informacijskih sustava tvrtki, a u našoj zemlji implementira ga tvrtka Megatrend poslovna rješenja (MPR). Riječ je o usluzi koja, uz sam nadzor sustava, pruža i mogućnost automatskog otklanjanja prijetnji s Interneta, obavješćivanje o neovlaštenom pristupu podacima, planiranje performansi i definiranje statusa svih resursa koje tvrtka nudi.

ARHITEKTURA QRADAR

IBM QRadar on Cloud ima modularnu arhitekturu koja se koristi za detekciju prijetnji i upravljanje sigurnošću. Može se dimenzionirati sukladno potrebama korisnika za prikupljanjem događaja (engl. Log) i tijekova (engl. Flow) podataka, te za analizu. Opseg funkcionalnosti rješenja IBM QRadar on Cloud može se proširiti dodavanjem modula kao što su QRadar Risk Manager, QRadar Vulnerability Manager i QRadar Incident Forensics. ◂

NEPRESTANO KORELIRANJE

IBM QRadar SIEM u IT okruženje tvrtke korisnika instalira se kao virtualno računalo (tzv. Log Collector) koje sve prikupljene nadzorne podatke, praktično u stvarnom vremenu, šalje u Megatrendov podatkovni centar, u kojem se nalazi centralni dio SIEM-ova rješenja. Svi događaji u korisnikovu informacijskom sustavu prate se na jasan i pregledan način, neprestanim "koreliranjem" – praćenjem svakog pojedinog događaja na svim uređajima i u svim aplikacijama, u svakoj mrežnoj točki, od njegova početka do kraja – preko naprednog *enginea* Sense Analytics. Ekspertni sustav koji to radi stalno je u kontaktu s IBM-ovom podrškom Watson o odlučivanju, povezuje sve tehničke detalje i sve prikazuje jasno i jednostavno, bez uporabe kompliciranih tehničkih kratica.

Naravno, u bilo kojem trenutku može se pogledati i svaka tehnička sitnica, ako vas zanima. Sustav IBM QRadar SIEM povezan je sa svjetskim sustavom X-Force "Threat Intelligence", gdje se automatski obrađuju i sprečavaju svi internetski napadi i otkrivaju anomalije u *online* prometu. Riječ je o opsežnom popisu potencijalno opasnih IP adresa koje služe kao "skladišta" raznih zlođudnih aplikacija, *spam* poruka i drugih internetskih prijetnji. IBM QRadar SIEM može se implementirati na tri osnovna načina – kao *cloud* usluga, kao samostalno rješenje na informacijskom sustavu tvrtke korisnika te hibridno, u kojem se dio resursa nadzire u oblaku, a dio na lokaciji korisnika. Kad se instalira kod korisnika, može se isporučiti kao softversko rješenje, i u kombinaciji s hardverom.

MEGATREND POSLOVNA RJEŠENJA

Tvrtka Megatrend poslovna rješenja d.o.o., kao IBM Platinum partner, do kraja ove godine imat će u svojoj ponudi i uslugu QRadar on Cloud. Istodobno će podržati i ostale načine implementacije usluge QRadar, ovisno o specifičnostima i potrebama korisnika. Sve informacije o tom proizvodu možete pronaći na mrežnim stranicama: www.megatrend.com ◂

ZAŠTITA IZ *CLOUDA*

Ovdje ćemo pobliže opisati varijantu QRadar on Cloud. Rješenje IBM QRadar on Cloud mrežna je inteligencija i analitička usluga koja otkriva napade na mrežnu infrastrukturu vaše tvrtke, tako da možete poduzeti sve potrebne obrambene korake prije nego što napad kojem ste izloženi napravi znatne štete ili izgubite važne podatke. Kao usluga temeljena na oblaku, IBM QRadar on Cloud, usmjerit će vas na stalni pregled nepravilnosti (gotovo u stvarnom vremenu) i zagušenja u mreži, a ne na nabavljanje i implementaciju tehnoloških komponenti koje su vam za to potrebne – troškovi instalacije hardvera i softvera smanjeni su na najmanju moguću mjeru.

Bit ćete stalno usmjereni na sigurnosnu analizu kratkog, upravljivog popisa sumnjivih i visoko vjerojatnih incidenata, s rješenjem koje je u potpunosti usklađeno sa svim regulatornim zahtjevima. IBM QRadar on Cloud može napraviti 1500 preddefiniranih izvještaja raznih vrsta, od izvještaja o izloženosti, do izvještaja o uskladivosti s propisima. Može kreirati EPS (Event per Second – događaj koji se generira na poslužitelju, aplikaciji ili uređaju i može se obraditi u određenu svrhu) i FPM (Flows per minute – tijek, zapis komunikacije između dva *hosta*) za više od pet stotina aplikacija i uređaja. Usluga obuhvaća i nadgledanje infrastrukture 24 sata na dan, 7 dana u tjednu, i primjenjivanje najnovijih razina softvera i kritičnih zakrpa kada one postanu dostupne.

VIŠE VRSTA INSTALACIJE

Osnovna instalacija (IBM QRadar on Cloud Basic Service) zapravo predstavlja

štita poslovanja tvrtke

klasičnu ponudu IBM SaaS, koja uključuje postavljanje početne *cloud* infrastrukture, kontinuirano nadgledanje te infrastrukture i održavanje softvera, obradu klijentskih zahtjeva za promjenama u sustavu i rješavanje problema te ima kapacitet od 1000 EPS za prikupljanje i obradu događaja dnevnika. Na tu uslugu mogu se nadograditi i fakultativne komponente (IBM QRadar on Cloud 1K EPS Upgrade), kojima se pruža dodatni kapacitet od 1000 EPS za prikupljanje i obradu događaja dnevnika. Klijent može kupiti više jedinica te nadogradnje, do maksimalne EPS razine koju ponuda podržava.

Sljedeća nadogradnja instalacije zove se IBM QRadar on Cloud 1K EPS Temporary Upgrade. Ta ponuda predstavlja nadogradnju usluge koja pruža dodatni kapacitet od 1000 EPS za prikupljanje i obradu događaja dnevnika, ali samo tijekom određenog broja mjeseci. Uz to, ta ponuda omogućuje ispunjavanje klijentskih zahtjeva za dodatnom pokrivenošću uslugom za vrijeme "skokova", tijekom godine, pomoću privremene nadogradnje kapaciteta. Na kraju razdoblja trajanja te ponude to privremeno povećanje kapaciteta uklonit će se iz klijentske okoline. Četvrta nadogradnja nosi naziv IBM QRadar on Cloud Data Capacity 1K EPS Upgrade. Riječ je o nadogradnji kapaciteta podataka kojom se dodaje dodatni prostor za pohranu i proširuju mogućnosti analize.

Nadogradnja kapaciteta pruža klijentima proširenje sustava za pohranu podataka u razdoblju od najviše jedne godine. Tvrtka korisnik može uzeti i dodatak: IBM QRadar on Cloud Flows Add-On, koji se jednostavno integrira s rješenjem IBM QRadar SIEM i s procesorima tijeka, radi pružanja preglednosti aplikacija i analize tijeka, što klijentu omogućuje zamjećivanje svih aktivnosti u cijeloj mreži, njihovo brže otkrivanje i bržu reakciju na njih. Tu je i još jedan dodatak, IBM QRadar on Cloud Flows Add-On, koji služi skupljanju i procesiranju podataka na samom ulazu u mrežu tvrtke korisnika.

Podaci se kontinuirano prenose u okolinu s *hostingom*, gdje su dostupni za uspostavljanje međuodnosa i prikazivanje na portalu. Skupljač obrađuje podatke vanjskog tijeka i pruža preglednost mreže na razini sloja 3. Dodatak za upravljanje ranjivostima – IBM QRadar on Cloud Vulnerability Management Add-On proaktivno primjećuje i otkriva sigurnosne ranjivosti mrežnog uređaja ili aplikacije, dodaje kontekst i podržava određivanje prioriteta aktivnosti kojima će se problem riješiti, a posljedice koje je izazvao, ublažiti. Više pojedinosti o svim navedenim funkcionalnostima možete pronaći na mrežnom odredištu na sljedećoj adresi: https://www.ibm.com/in-en/marketplace/hosted-security-intelligence

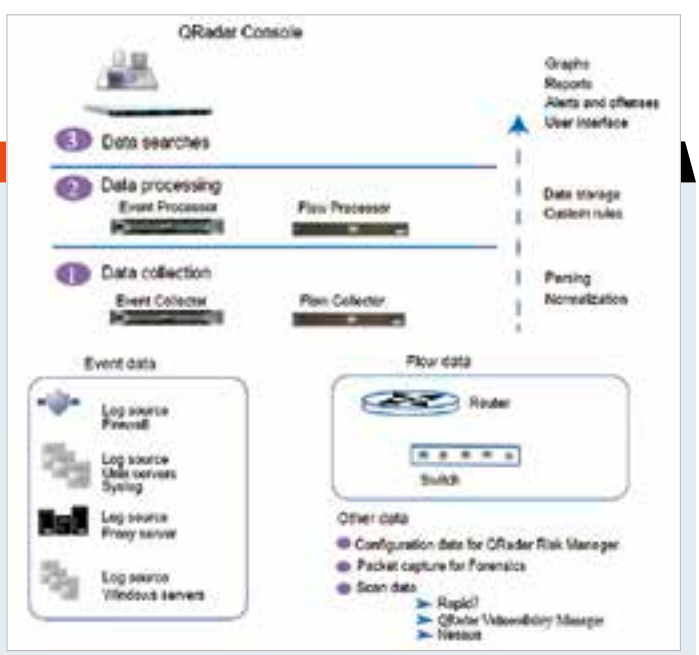
TRI SLOJA

Platforma QRadar on Cloud sastoji se od tri sloja. Prvi sloj je prikupljanje podataka. U njemu se prikupljaju događaji i tijekovi podataka. Događaj je nešto što se dogodi u nekom određenom trenutku, na nekom uređaju ili aplikaciji koja se nalazi u korisničkoj okolini, nešto kao, primjerice, logiranje korisnika, *e-mail*, VPN konekcija, proxy konekcije, *firewallsko* odbijanje i tome slično. Događaj se generira na poslužitelju, aplikaciji ili uređaju, i može se obraditi za određenu svrhu. Tijek je zapis komunikacije između dva *hosta*. Svi paketi koji sadrže isti izvorni IP, odredišni IP, izvorni *port*, odredišni *port* i protokol, spajaju se u jedan zapis tijeka. Drugi sloj je obrada podataka. Na tom sloju događaji i tijekovi podataka obrađuju se sukladno definiranim pravilima i pohranjuju. Rezultati obrade predstavljaju pregled sigurnosnih prijetnji ili prekršaja, i na temelju njih se kreiraju sigurnosna upozorenja. Treći sloj platforme QRadar on Cloud je pretraživanje podataka. Tu se radi pretraživanje podataka, analiza, izvještavanje i istraživanje prijetnji ili prekršaja. ◂

QRADAR KOMPONENTE

Osnovne komponente rješenja QRadar on Cloud su:

- **QRadar Console** – predstavlja korisničko sučelje koje omogućuje pregled događaja, tijekova, izvještaja, prijetnji i administrativne funkcije
- **QRadar Event Collector** – prikuplja podatke o događajima iz lokalnih ili udaljenih resursa te formatira podatke u format prikladan za daljnju obradu i šalje ih Event Processor.
- **QRadar Event Processor** – obrađuje podatke sukladno definiranim pravilima (Custom Rule Engine). Ako obrada rezultira uparivanjem podataka s određenim pravilom za obradu, Event Processor izvršava aktivnost definiranu tim pravilom. Event Processor može pohranjivati podatke lokalno ili na Data čvor.
- **QRadar Flow Collector** – prikuplja tijekove podataka koristeći sučelje SPAN (Switch Port Analyzer port) ili sučelje TAP (Test Accessing Point). QRadar Flow Collector ima mogućnost prikupljanja podataka s eksternih izvora tijekova podataka (primjerice, NetFlow).
- **QRadar Flow Processor** – obrađuje tijekove podataka. Također ima mogućnost prikupljanja podataka s eksternih izvora (NetFlow, J-Flow i sFlow), kao i direktno s usmjerivača u vlastitoj mreži.



- **QRadar Data Node** – omogućuje sustavu s implementiranim QRadarom dodavanje spremišta podataka i povećanje kapaciteta obrade podataka, ovisno o zahtjevu korisnika. Data Node omogućuje povećanje brzine obrade podataka tako da se osiguraju dodatni hardverski resursi. ◂