EventTracker lancerer Security Center 8.3 og udvider dermed funktionerne i forbindelse med trusselsintelligens og ransomwarebekæmpelse betydeligt

Juni, 2017

EventTracker har netop annonceret lanceringen af EventTracker Security Center 8.3, som er den seneste version af den prisvindende EventTracker SIEM platform.

Den nye version indeholder avancerede funktioner til bekæmpelse af moderne ransomware såvel som polymorf og muterende malware, en udvidet integration af trusselsintelligensmæssige funktioner samt forskellige GUI forbedringer, der samlet betyder, at man er i stand til at opdage trusler hurtigere.

Den omfattende EventTracker Security Center 8.3 platform indeholder SIEM, intrusion detection, vulnerability scanning, trusselsintelligens og honeynet deception teknologi og implementeres enten on-site eller i skyen.

Security Center 8.3 platformen udgør desuden kernen i EventTracker's SIEM-as-a-Service tilbud, SIEMphonic. Virksomheden sikrer sine kundes succes ved at oven på teknologien at lægge lag af profesionelle services til remote administration, analyse, compliance understøttelse og nye muligheder for indstillinger, som sikrer optimale resultater.

EventTracker er ni år i træk optaget i Gartner Research's Magic Quadrant for SIEM.

De vigtigste funktioner i EventTracker Security Center 8.3 er:

- **Dormant Malware Hunter** — Moderne malware, herunder ransomware, kopierer sig selv med forskellige navne og hashes til forskellige foldere, så selv om originalen identificeres og fjernes, er klonerne stadig klar til at angribe på et senere tidspunkt. Dormant Malware Hunter identificerer skjulte EXE og DLL filer, der aldrig er eksekverede, og udelukker dem, der ligger i kendte, sikre fil lister. Dermed kan kopier af malware fjernes fra netværket, så man undgår en gentagelse eller spredning af et angreb.
- **Threat Center STIX/TAXII understøttelse** — EventTracker's trusselsbekæmpelsesfunktioner er betydeligt udvidet gennem integrationen af kommercielle og open source trussels-feeds og intelligence fra STIX/TAXII-kompatible leverandører, såvel som fra kundernes egne interne honeynet. Threat Center bruger disse data til at reducere falske positiver og finder og prioriterer samtidig potentielle og faktiske trusler.
- **Forbedret MSP brugeradministration** – Et vigtigt fokus i denne version er at IT service leverandrører bedre kan beskytte deres kunders infrastruktur med forbedret skalerbarhed og brugeradministration for Managed Service Providers (MSPs), fordi man kan håndtere abonnementsrelaterede aktiviteter for hver enkelt kunde, som fx at spore det månedlige forbrug af services. Det er også nemmere at overvåge forbruget for flere kunder og det er muligt at administrere brugertilladelser mere detaljeret.
- **Forbedret brugergrænseflade i EventVault Explorer** – Det opgraderede interface indeholder hurtigere dataindlæsning, større udvælgelseskontrol, og en enklere brugeroplevelse for MSPs , der bruger EventVault Explorer. Explorer funktionaliteten gør det nemmere at søge efter logs og hurtigere at søge efter specifikke data og gemme søgekriterier til senere brug.

De nye opgraderede funktioner i Security Center 8.3 forbedrer virksomhedens netværkssikkerhed og bevidsthed om eksterne trusler betydeligt. Dette er særligt kritisk, da mere end 90% af alle cyber

angreb ifølge den såkaldte *2017 Verizon Data Breach Investigations Report* kommer fra eksterne trusselsaktører.

“I en verden hvor mængden af cyber angreb hele tiden øges, er det blevet altafgørende for virksomheder hurtigt og nemt at kunne vurdere digitale trusselsbegiveheder, når de skal beskytte sikkerheden i deres infrastrukturer” udtaler A.N. Ananth, der er CEO i EventTracker. “De nye funktioner i Security Center 8.3 giver et hidtil uset niveau af trusselsintelligens på et ekstremt højt evalueringsniveau, forbedrer muligheden for at opdage trusler betydeligt og er samtidig nemmere at arbejde med for MSPs.”