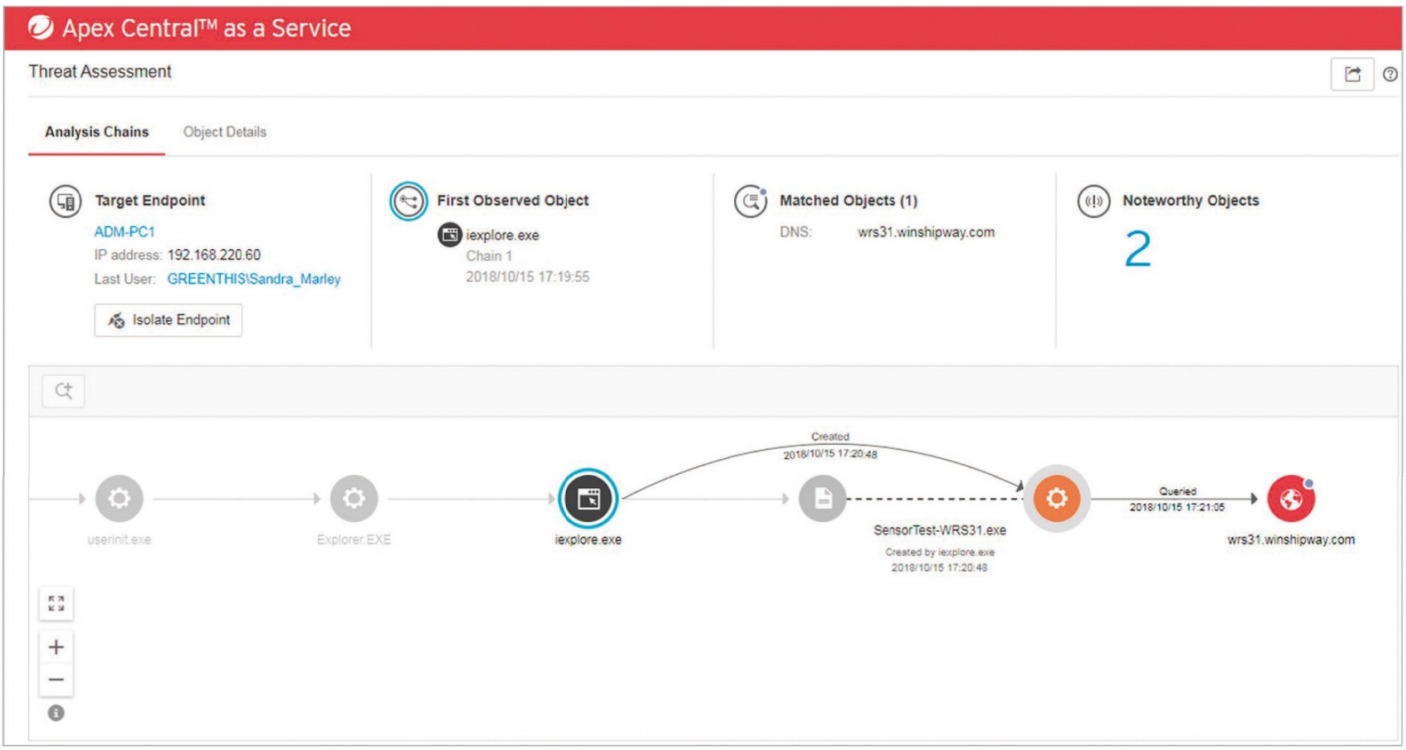


Slika koja će i manje upućenoj osobi u nadzoru sustava reći gotovo sve. Vidi se cijeli vremenski obilježen tijek incidenta, s polaznim i ciljanim datotekama i svim posljedicama koje su iz toga proizašle

Virtualni CSI

U procesu sukcesivne aproksimacije na putu prema nedostižnom idealu stopostotne sigurnosti informacijskih sustava, Trend Micro počastio nas je novim alatom imena Endpoint Detection and Response. EDR se obradom incidenata prouzročenih malicioznim kôdom bavi korištenjem dubokih forenzičkih metoda, zadirući pritom u daleku povijest upotrebe štićenih računala kako bi nas što učinkovitije štitio od prijetnji koje u trenutku nastanka nisu bile poznate

Trend Micro Endpoint Detection and Response

\+ Impresivna detaljna analiza s preciznim opisima svih radnji koje je maliciozni kôd pokušao poduzeti

– Nema očitih nedostataka

Dojam: Vrlo zanimljivo rješenje za sve paranoike koje će vašu mrežnu sigurnost osjetno unaprijediti i podići je na višu razinu

Cijena **26.76 eura** po korisniku bez PDV-a

Ustupio Veracomp, www.veracompadria.com

Rajko Plečko

Ozbiljnim pristupom borbi protiv svih vrsta mrežnih ugroza, tvrtka Trend Micro u svojih se nešto više od trideset godina postojanja uspješno pozicionirala u sam vrh među zvučnim imenima vendora koji se bave Endpoint Protection platformom i Intrusion Detection and Prevention uređajima i alatima, pa ju iz godine u godinu možemo naći u gornjem desnom polju Gartnerovog "magičnog kvadranta". Za one koji se ne zamaraju takvim reportima, to znači da su označeni kao vizionari i "top performeri", što svakako govori o ozbiljnosti kompanije i njezinih proizvoda.

Endpoint Discovery and Response (EDR) jedan je od novih alata prije svega namijenjenih *enterprise* okolini, ali ako vodite i neki manji biznis, koji se većim dijelom oslanja na informacijske tehnologije te u kojem baratate osjetljivim i vrijednim podacima, EDR će vam biti od značajne pomoći u svakodnevnoj borbi protiv virtualnih ugroza.

KAKO POČETI

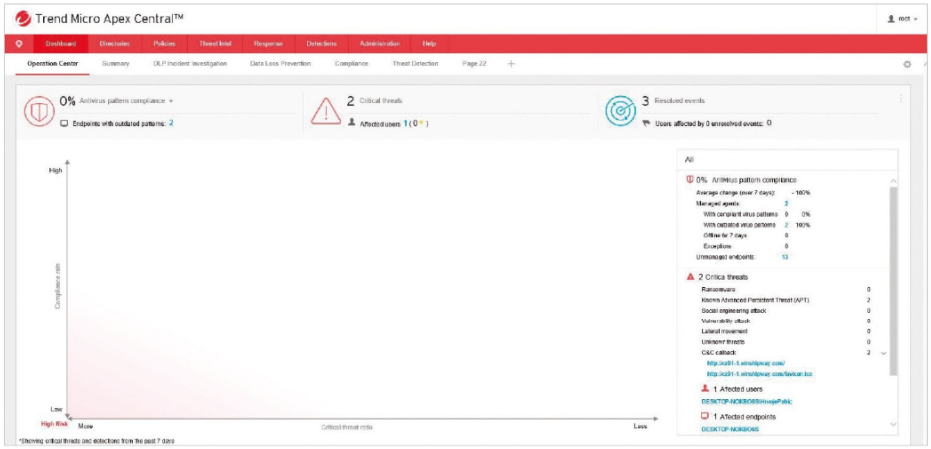
EDR je softver za čiju instalaciju i puštanje u pogon moramo zadovoljiti određene uvjete koji većini tvrtki neće predstavljati veću prepreku. Potrebna su nam, naime, dva servera s Windows Server OS-om i SQL baza. Na jednom serveru nalazi se Apex One, a na drugom Apex Central. Serveri će u današnjem svijetu gotovo sigurno biti virtualni na infrastrukturi koju već imamo, a ni SQL nije neka posebna egzotika, pa će biti dovoljna još jedna instanca koja će se baviti podacima generiranim za EDR. Što se tiče hardverskih zahtjeva, bit će dovolj-

ne dvije ili četiri jezgre i 8 GB RAM-a po virtualnom stroju.

Današnje IT prijetnje dizajnirane su da zaobiđu tradicionalne sigurnosne alate te neopaženo udu u sustav i kompromitiraju ga, s ciljem izazivanja ozbiljnih poslovnih i financijskih posljedica za organizaciju, ili jednostavno da bi se iskoristili tuđi resursi za buduće napade na neki treći sustav, prema želji administratora komandnog centra. Zadatak djelotvornog EDR rješenja za detekciju i odgovor na prijetnje jest uočiti ih i eliminirati pravodobnom reakcijom prije nego što kompromitiraju bitne podatke organizacije. Trend Micro u okviru rješenja za zaštitu krajnjih točaka Apex One nudi Endpoint Sensor – tehnologiju poznatu kao EDR, dodatni sloj zaštite koji bilježi i prati neovlaštene aktivnosti, otkriva izvor zaraze (IoC) te omogućuje pravodobnu reakciju, s ciljem onemogućavanja lateralnog kretanja i širenja prijetnje.

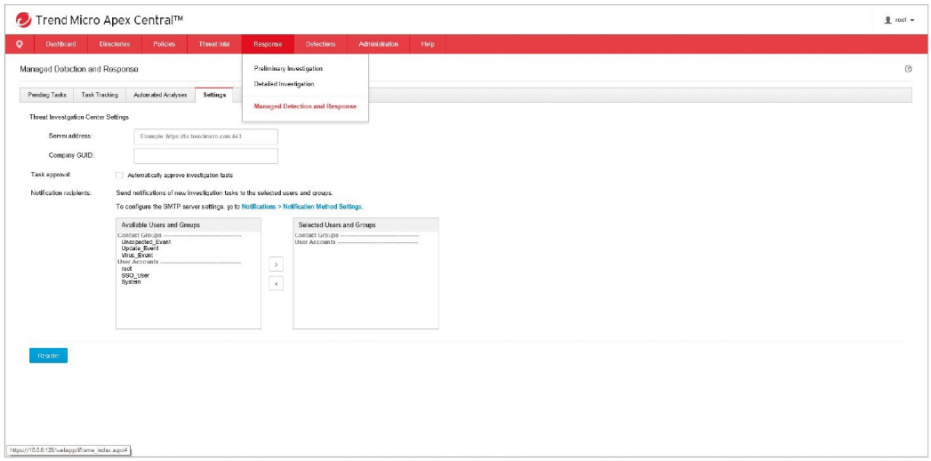
EDR funkcionira tako da se sve aktivnosti koje se događaju na korisničkoj strani spremaju kao metapodaci za kasniju analizu. Spremaju se promjene u Windows Registryju, povijest pristupanja web-stranicama, popis datoteka koje su se izvršile, i mnogo drugih. Sve to kasnije omogućuje detaljnu forenziku nad svim klijentskim računalima i otkrivanje izvora i uzroka te eliminaciju posljedica incidenta.

Svi prikupljeni metapodaci periodično se zapisuju u centralnu bazu te se u stvarnom vremenu uspoređuju s bazama malicioznih mrežnih stranica, nakon čega se donosi odluka može li se ili ne pristupiti pojedinoj lokaciji. No, ako nam EDR i dozvoli pristup, to ne znači da lokacija pouzdano nije maliciozna, nego da u tom trenutku o njoj nemamo takvu informaciju. Dakle, ako u nekom trenutku namjernim ili slučajnim posjetom nekoj od rizičnih stranica skinemo dosad nepoznati maliciozni kôd koji je našem antivirusnom sustavu prošao "ispod radara", to ne znači da su posljedice ireverzibilne te kako uzroku više nećemo moći ući u trag. Kad sustav bude raspolagao informacijom o malicioznoj mrežnoj lokaciji ili prijetnji koja je kod nas već izazvala posljedice, o tome će nas detaljno obavijestiti i ponuditi nam mogućnost podrobne analize. Moći ćemo vidjeti kompletan vremenski označen proces koji je nakon toga uslijedio te sve uređaje na koje je djelovao. Tu imamo mogućnost zatražiti od EDR-a da pokrene svoj "vremenski stroj", vrati se u prošlost te eliminira prijetnju, ali i sve posljedice koje je izazvala na sustavu, a koje više i ne moraju biti očite. Cijeli opisani proces vidljiv je u tabličnom prikazu, a svaki odabrani još i u grafičkom, iz kojeg je i manje stručnom oku jasan izvor, cilj i tijek incidenta te koraci koji su mu na raspolaganju u suzbijanju posljedica. Korisnik može odlučiti kojim će putem krenuti dalje. Može zaustaviti objekt zaraze, poslati informacije svim korisničkim računalima vezano uz pronađene datoteke u obliku antivirusne definicije i/ili detaljno provjeriti proizvoljna korisnička računala.



Kontrolna ploča sustava iz kojeg imamo pregled nad svim detektiranim pojavama te možemo odlučiti o daljnjim postupcima

Sakupljanje i čuvanje povijesnih podataka potrošit će na svakom štićenom sustavu oko 2 GB diskovnog prostora mjesečno, a kako se svi ti metapodaci periodički upisuju u SQL bazu i tamo čuvaju šezdesetak dana, jednostavna matematika (ovisno o broju klijenata) pokazat će o kolikoj se količini diskovnog prostora radi.



Trenutak odluke nakon uočenog incidenta. Preliminarno istraživanje, detaljno istraživanje ili MDR

MANAGED DETECTION AND RESPONSE (MDR)

Ako vam ne odgovara da za konstantni nadzor rada ovog sustava koristite vlastite ljudske resurse ili nemate ljude s potrebnim znanjem i vještinama, vama je namijenjen Managed Detection and Response (MDR). Tu uslugu možete kupiti od Trend Micra pa će cijeli posao za vas odraditi njihov Security Operation Center (SOC). Korisniku je omogućen izbor do koje razine želi automatizaciju od Trend Micro SOC-a. Princip rada reguliran je kroz dozvole u obliku dozvola (IT *approval flag*), gdje se detaljno može odabrati do koje razine administrator sustava ne mora odobravati promjene.

Treba reći da cijela ova priča također može biti smještena u *cloudu,* što će vas potpuno osloboditi brige o hardveru, instalaciji i nadzoru sustava.