Využitím riešenia **Trend Micro Deep Discovery Inspector (Virtual Appliance)** dôjde k jednoznačnému rozpoznaniu, určeniu a identifikácii hrozieb v reálnom čase a poskytnutie hĺbkovej analýzy, určeniu krokov, ktoré sú potrebné na zabránenie, odhalenie a ovládnutie útokov na infraštruktúru vašej spoločnosti.

Spôsoby, metódy testovania

Deep Discovery Inspector musí byť nasadený v SPAN (Switch Port Analyzer) alebo TAP móde. To znamená, že Deep Discovery Inspector musí byť pripojený do SPAN portu sieťového prepínača (switcha) alebo do sieťového TAP. V tomto režime je celá sieťová prevádzka zrkadlená alebo kopírovaná do Deep Discovery Inspectora čo umožňuje jej neinvazívnu analýzu.

Spôsoby a metódy fungovania testov

	Detekcia útoku	**Metóda detekcie**
Škodlivý obsah (malicious content)	Emailová správa obsahujúca exploit v priloženom dokumente napr. •Drive-by downloads •Zero-day alebo známy malware	Dekóduje a rozbalí priložené súbory • Simulácia spustenia podozrivých súborov v sandboxe • detekcia exploitu • Malware scan *(metóda signatúr & Heuristická metóda)*
Podozrivá komunikácia (Suspect Communication)	Zachytená C&C komunikácia a malware: bots, downloaders, data stealing, worms... • Backdoor aktivita útočníka	Analýza destinácie - cieľa (URL, IP, doména, email, IRC kanál, …) cez dynamický blacklisting, white listing • všetky požiadavky a priložené URL sa vyhodnotia pomocou Smart Protection Network
Správanie útočníka (attack behavior)	Malware aktivity: šírenie, sťahovanie , spammovanie, … • Aktivity útočníka: scanovanie, brute force, tool download , … •exfiltrácia dát	Heuristická analýza •Identifikácia a analýza použitia viac než 80 protokolov a aplikácii vrátane http aplikácií

Výstupmi monitorovania je:

- Odhalenie cielených útokov na IT infraštruktúru spoločnosti – poskytne prehľad o celej sieti, detailné informácie i nástroje potrebné k účinnému boju s hrozbami APT a cielenými útokmi;
- Detekcia a identifikácia hrozieb v reálnom čase, následná hĺbková analýza a ponuka informácií, ktoré spoločnosť potrebuje na vyhodnotenie rizík a realizáciu nápravných krokov;
- Hĺbková kontrola obsahu sieťovej prevádzky naprieč viac ako 80+ protokolmi a aplikáciami
- Detekcia a ochrana spoločnosti pred týmito hrozbami:
  - Hrozby APT a cielené útoky

  - Zero-day malware a exploity zneužívajúce dokumenty
  - Sieťová aktivita útočníka
  - Webové hrozby (exploity, nevedomé downloady)
  - E-mailové hrozby (phishing, spear phising)
  - Krádeže dát
  - Botnety, trójske kone, červy, keyloggery
  - Nebezpečné (disruptívne) aplikácie
- Hĺbková kontextová analýza a odozva – zrýchľuje obnovu na základe doporučení a exportu aktuálnych bezpečnostných informácií ;
- Zníženie rizika zničenia a straty dát;
- Ochrana pred aplikačnými útokmi a zero day útokmi už na úrovni perimetra;
- Sledovanie anomálií v sieťovej prevádzke a odhaľovanie infikovaných zariadení;
- Ochrana pred škodlivým webovým obsahom, web-reputačné databázy, filtrovanie a blacklisting;