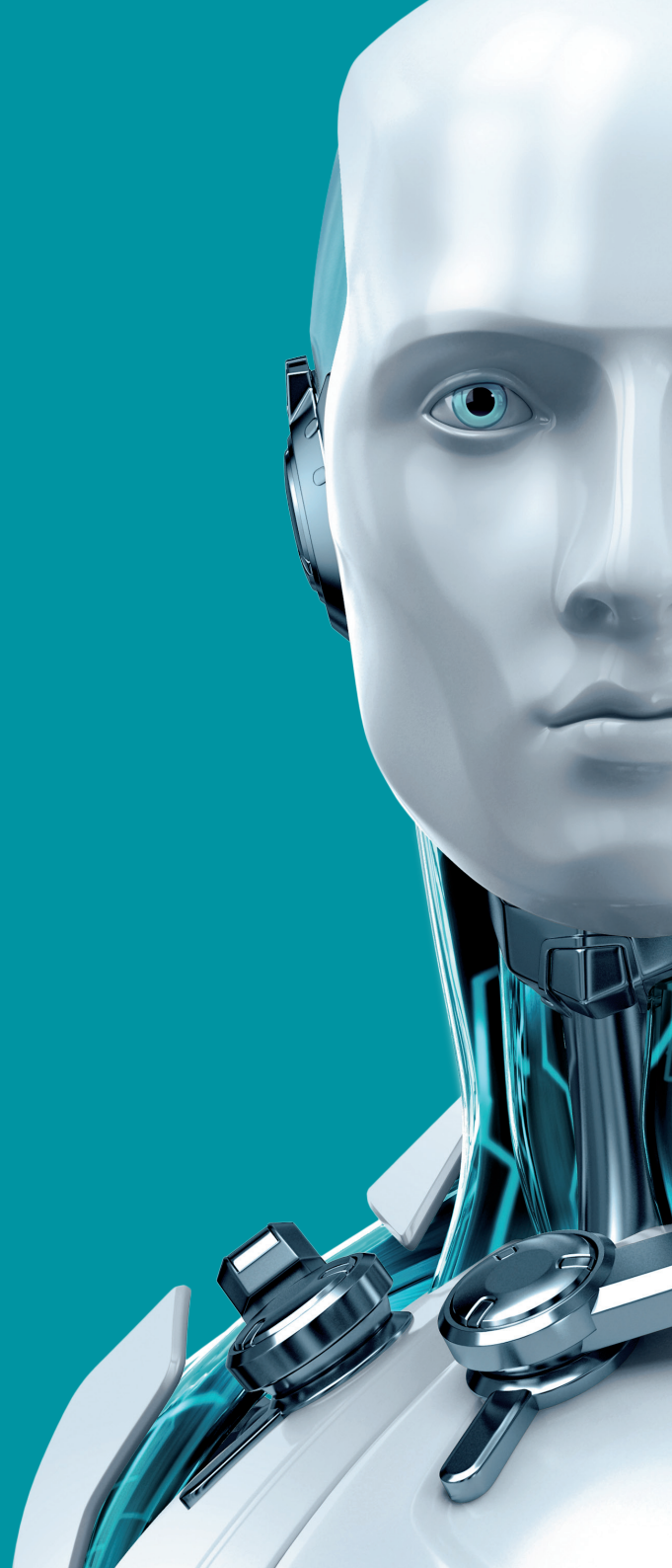
GREYCORTEX MENDEL

Analýza sieťovej prevádzky

Prehľad produktu

BIZNIS

ESET TECHNOLOGICKÁ ALIANCIA



GREYCORTEX MENDEL

Analýza sieťovej prevádzky s GREYCORTEX MENDEL

GREYCORTEX MENDEL je riešenie určené na hĺbkovú analýzu sieťovej prevádzky, monitorovanie výkonu, detekciu hrozieb a zabezpečenie kompletného prehľadu o sieti v rámci podnikov, vládnych inštitúcií a sektora kritickej infraštruktúry. MENDEL využíva vyspelú umelú inteligenciu, strojové učenie a analýzu veľkých dát (tzv. big data), vďaka čomu pomáha organizáciám udržiavať IT infraštruktúru zabezpečenú a spoľahlivú.

MENDEL nie je len ďalším nástrojom na monitorovanie správania v rámci siete. Kombinuje analýzu hrozieb, strojové učenie, umelú inteligenciu, kontrolu paketov, koreláciu udalostí a ďalšie nástroje s cieľom identifikovať podozrivú aktivitu v sieti. Toto umožňuje IT bezpečnostným tímom odhaľovať hrozby s väčšou istotou a zasiahnuť rýchlejšie ako v prípade tradičných riešení sieťovej bezpečnosti.

Identifikujte hrozby ešte pred vznikom škôd

Mnoho iných poskytovateľov sa zameriava na známe techniky útokov alebo vzorky škodlivého kódu. Vďaka pokročilým metódam umelej inteligencie riešenie MENDEL prekračuje hranice známych hrozieb, keďže deteguje a rozpoznáva príznaky škodlivého správania už na tej najnižšej úrovni. Hrozby sú vďaka tomu identifikované už v počiatočných fázach, čo znižuje čas reakcie na incidenty, predchádza ďalším škodám a znižuje celkové bezpečnostné riziko.

MENDEL v sebe tiež integruje detekciu na základe databázy vzoriek (signatúr) a poznatky o známych hrozbách – tým sa zvyšujú detekčné schopnosti a zároveň znižuje počet nesprávnych detekcií (tzv. falošných poplachov).

8 – 16 hodín
Čas, ktorý útočník potrebuje na to, aby prenikol do siete.

8 mesiacov
Priemerný čas prítomnosti pokročilej pretrvávajúcej hrozby (APT) v sieti obete bez toho, že by bola zachytená.

98 dní
Priemerný čas, ktorý je potrebný na zachytenie APT útoku.

71 %
Percento organizácií, ktoré útok samy nezachytia.

Automatické prispôsobenie

Jedinečný mechanizmus NBA (Network Behavior Analysis) riešenia MENDEL slúži na analýzu správania siete a využíva pokročilú matematickú analýzu v rámci strojového učenia na vytváranie a prispôsobovanie pravidiel detekcie podľa predchádzajúcich sieťových prenosov. Integruje tiež vstupy z ostatných detekčných mechanizmov a zahŕňa špecializované algoritmy, ktoré okrem iného dokážu aj rozlišovať medzi strojovým a ľudským správaním. Mechanizmus NBA v rámci produktu MENDEL je jediným riešením na trhu, ktoré ponúka túto schopnosť.

Citlivejšia detekcia

Protokol ASNM (Advanced Security Network Metrics) je založený na pokročilých sieťových metrikách a umožňuje riešeniu MENDEL monitorovať viac ako 70 atribútov každého jedného toku v sieti. Vďaka takejto analýze na pokročilej úrovni je MENDEL v porovnaní s inými súčasnými riešeniami na trhu efektívnejší pri detekcii škodlivého správania a ostatných hrozieb.

Pokročilé techniky analýzy dát (tzv. data mining) umožňujú riešeniu MENDEL spracovať niekoľkonásobne viac informácií o sieťovej prevádzke a viac atribútov dátových tokov ako riešenia založené na NetFlow protokoloch, navyše v reálnom čase. Okrem toho MENDEL dosahuje rýchlosť až 10Gb/s v rámci konfigurácie s jednou sieťovou sondou a jedným kolektorom a až 40Gb/s v prípade kolektora.

MENDEL zachytáva skryté hrozby:

- malvér na mobilných a vstavaných zariadeniach,
- úniky údajov pomocou DNS, SSH, HTTP(S) a podobne,
- „tunelované" sieťové prenosy,
- protokolové anomálie,
- útok typu „maškaráda" (útočník sa vydáva za niekoho iného),
- detekcia spamu,
- príprava na krádež dát a ich exfiltráciu (získavanie dát),
- automatizovaný zber dát,
- krádeže dát,
- phishingové útoky.

Lepšie monitorovanie výkonu

MENDEL poskytuje podrobné informácie o výkone aplikácií z pohľadu používateľa aj siete. Riešenie nevyužíva agentov a ponúka možnosť monitorovať každý jeden dátový tok, naprieč rôznymi typmi aplikácií. Všetky dátové toky sa zobrazujú v širokej škále vizualizácií s rozličnými možnosťami triedenia a filtrovania. Tímy tak majú k dispozícii podrobné informácie, aby mohli chrániť a optimalizovať kľúčové procesy, ako aj využiť možnosť jednoduchej a rýchlej analýzy príčin vzniku – v reálnom čase. To znamená, že organizácie pozorujú nielen zlepšenie v rámci bezpečnosti, efektivity a prehľadnosti siete, ale aj návratnosť svojej investície.

Jednoduchosť používania bez spomalenia siete

Riešenie MENDEL nie je len o pokročilých nástrojoch, metódach a schopnostiach. Rýchlo ho nasadíte, šetrí vám čas pri administratíve a zozbierava dáta bez spomalenia rýchlosti siete. MENDEL sa medzi IT manažérmi teší veľkej obľube z nasledujúcich dôvodov:

- Inštalácia riešenia MENDEL a konfigurácia základných nastavení trvá 30 minút. MENDEL preskúma sieť a mechanizmus IDS začne okamžite hlásiť výsledky. Praktické výstupné dáta sú dostupné po siedmich dňoch a kompletný cyklus učenia mechanizmu NBA sa dokončí do 28 dní.
- Vytváranie správ a rozpoznávanie identifikovaných hrozieb je s riešením MENDEL jednoduché, keďže ponúka rozšírené možnosti filtrovania a triedenia, prispôsobenia správ a intuitívne webové rozhranie, ktoré taktiež šetrí váš čas.
- MENDEL sieťovú prevádzku monitoruje a vizualizuje bez rušivého vplyvu, pričom zaznamenáva informácie o každom dátovom toku. To znamená, že používatelia môžu ľahko identifikovať každý dátový tok v reálnom čase a zistiť, kto používa konkrétne služby, sieťové uzly a šírku prenosového pásma. Riešenie posudzuje výkon aplikácií a siete a vykonáva analýzu príčin vzniku bez negatívneho vplyvu na čas odozvy siete.

Prepojenie analýzy správania siete a strojového učenia

Mechanizmus NBA, ktorý je súčasťou riešenia MENDEL, využíva pokročilú matematickú analýzu v rámci strojového učenia, metódy klasifikácie s/bez učenia z tréningových dát, zhlukovanie (clustering) a analýzu anomálií:

- modely normálneho správania v rámci siete, všetkých podsietí, hostiteľov, služieb a jednotlivých dátových tokov,
- Bayesová analýza zmenených atribútov,
- pravdepodobnostné zmiešané modely (Gaussov EM algoritmus),
- rozličné ad hoc techniky.

O spoločnosti GREYCORTEX

GREYCORTEX používa vyspelú umelú inteligenciu, strojové učenie a hĺbkovú analýzu dát (data mining). Pomocou týchto metód pomáha organizáciám udržiavať IT operácie zabezpečené a spoľahlivé. MENDEL je riešenie na analýzu sieťovej prevádzky vyvinuté spoločnosťou GREYCORTEX, ktoré pomáha podnikom, vládnym inštitúciám a sektoru kritickej infraštruktúry zabezpečiť si ochranu a detegovať kybernetické hrozby ohrozujúce citlivé údaje, siete, obchodné tajomstvá a reputáciu, pričom iné produkty sieťovej bezpečnosti takúto detekciu nemajú.

Spoločnosť GREYCORTEX nazvala svoj softvér „MENDEL" na počesť Gregora Johana Mendela, otca modernej genetiky, ktorý svoje vedecké objavy urobil v českom meste Brno, kde GREYCORTEX sídli.

TECHNOLOGICKÁ ALIANCIA

ESET Technologická Aliancia má za cieľ lepšie chrániť firemných zákazníkov pomocou doplnkových IT bezpečnostných riešení. Prinášame našim klientom nové možnosti na zaistenie maximálnej bezpečnosti v neustále sa meniacom prostredí. Našu overenú technológiu kombinujeme s ďalšími produktmi, ktoré vo svojej kategórii vynikajú vysokou kvalitou.

Technické informácie

Architektúra	Architektúra riešenia MENDEL je tvorená sieťovými sondami a kolektormi. Sondy slúžia na detekciu známych hrozieb a dodávanie dát o sieťovej prevádzke mechanizmu NBA v rámci kolektora. Kolektory slúžia na premenu zozbieraných dát (metrík) na informácie. Sondy riešenia MENDEL podporujú rýchlosť do 10Gb/s a kolektory zvládnu až 40Gb/s. Rozsiahle nasadenia naprieč viacerými lokalitami využívajú kolektor, ktorý dokáže pokryť 10 a viac sieťových sond (fyzických aj virtuálnych).
Vstup	Vstupmi sú sieťové toky dát dodávané metódou SPAN (zrkadlenie portov) alebo TAP, reputácie IP adries (napr. známe botnety), zdroje spamu, uzly TOR, proxy servery a ďalšie informácie.
Výstup	Výstupy sú dostupné vo webovom rozhraní a ako stiahnuteľné .pcap súbory. Prispôsobené správy sa dajú poslať na e-mail vo formáte .pdf a .doc. Výstupy sa tiež dajú exportovať do systémov SIEM vo formáte CEF alebo IDEA.
Implementácia	GREYCORTEX MENDEL je možné implementovať ako hardvérové zariadenie („appliance") alebo s určitými obmedzeniami aj ako virtuálne zariadenie. Medzi ďalšie možnosti patrí implementácia riešenia MENDEL v prostredí SECaaS, v rámci modelov bezpečnostných operačných centier (SOC) alebo ako jednorazový bezpečnostný audit siete klienta.
Nasadenie	**Jednoduché nasadenie:** MENDEL je možné nasadiť ako jednu sieťovú sondu a kolektor na jednom zariadení („appliance"). **Rozložené nasadenie:** MENDEL je možné nasadiť použitím viacerých kolektorov a sond zdieľajúcich informácie o sieťovej prevádzke a hrozbách, čo umožňuje monitorovať geograficky odľahlé lokality a/alebo spracúvať veľké objemy sieťových dát.