ESET TECHNOLOGY ALLIANCE

GREYCORTEX

Detekcia sieťových hrozieb a reakcia

Progress. Protected.

TECHNICKÁ ŠPECIFIKÁCIA

Mendel, riešenie na detekciu sieťových hrozieb a reakciu na ne od nášho partnera GREYCORTEX, ktorý je členom ESET Technology Alliance, poskytne vašej organizácii podrobný prehľad o sieti, pokročilú detekciu hrozieb a spoľahlivé možnosti reakcie vďaka integrácii s XDR.

Riešenie umožňujúce detekciu sieťových hrozieb a reakciu na ne je základným nástrojom používaným v podnikoch, vo vládnych inštitúciách a v sektore kritickej infraštruktúry: Mendel monitoruje a analyzuje sieťovú komunikáciu, pomáha odhaľovať známe aj neznáme hrozby vrátane únikov údajov, prevádzkových anomálií, škodlivých aktivít zamestnancov a ďalších ťažko odhaliteľných hrozieb. Vďaka využitiu zrkadlenej komunikácie z chrbticových prepínačov poskytuje Mendel podrobný prehľad o celej monitorovanej sieti. Dá sa nasadiť v priebehu niekoľkých minút a dopĺňa tradičné bezpečnostné nástroje, čím znižuje čas a zdroje potrebné na zaistenie bezpečnej a spoľahlivej sieťovej prevádzky.

JEDINEČNÝ PREHĽAD

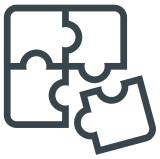
o vašich IT a OT sieťach

- Prehľad o všetkých zariadeniach a používateľoch v sieti
- Vizualizácia všetkých ich komunikácií – až na úrovni aplikácie
- Monitorovanie správania zariadení BYOD a IoT
- Identita používateľa, označovanie zariadení a podrobnosti o inventári
- Monitorovanie výkonnosti aplikácií, zariadení a siete
- Zaznamenávanie a dešifrovanie komunikácie
- Podpora softvérovo definovaných sietí (SDN)/Cisco ACI
- Reportovanie zohľadňujúce historický kontext

ÚČINNÁ DETEKCIA

hrozieb a anomálií v počiatočných štádiách

- Počítačová kriminalita, aktivity hackerov, ransomvér, nedetegovaný malvér
- Overenie funkčnosti firewallu, zabezpečenia koncových zariadení alebo siete VPN
- Nesprávna konfigurácia a zmeny v nastaveniach siete
- Porušenie bezpečnostnej politiky
- Viaceré metódy detekcie správania vrátane strojového učenia bez učiteľa, štatistickej analýzy a korelácie udalostí
- Informácie o hrozbách a podpisy IDS
- Analýza zašifrovanej komunikácie
- Analýza pomocou plne filtrovateľných údajov s viacerými možnosťami zobrazenia



JEDNODUCHÁ INTEGRÁCIA S XDR

vďaka integrácii EDR, firewallov a ďalších modulov

- Maximálny prehľad o celej infraštruktúre
- Korelácia medzi detekciami škodlivej komunikácie
- Prioritný zoznam podozrivých detekcií a zraniteľných konfigurácií
- Rýchla identifikácia základnej príčiny problémov
- Minimalizácia času potrebného na reakciu na incident
- Automatické blokovanie nežiaducej komunikácie
- Preposielanie údajov, upozornení a udalostí do platformy XDR, nástrojov SIEM alebo SOAR
- Zlepšenie efektivity práce tímov zaisťujúcich dohľad nad bezpečnosťou

Metódy detekcie

PREDIKČNÁ ANALÝZA

Spoznajte a predvídajte správanie siete vrátane všetkých podsietí, hostiteľov a služieb na každom hostiteľovi. Všetka komunikácia, ktorá nie je v súlade s naučenými modelmi správania, je hlásená ako anomálna (napr. anomálny prenos dát, objem komunikačných partnerov, počet komunikujúcich portov, počet tokov, trvanie komunikácie, čas komunikácie atď.). Mendel upravuje svoj model správania siete každú hodinu.

ANALÝZA ZISTENÍ

Mendel používa vždy aktuálny zoznam aktívnych služieb a hostiteľov. Ak sa v monitorovanom segmente siete objaví nový hostiteľ (napríklad BYOD) alebo služba, táto udalosť sa nahlási. Rovnaká metóda sa používa, keď služby alebo hostitelia prestanú komunikovať, zmenia svoje MAC adresy alebo keď sa zmenia názvy DNS. Mendel takisto reportuje všetku komunikáciu medzi povolenými a zakázanými službami na základe prednastavených politík.

ANALÝZA TOKOV

Analýza známych a nežiaducich vzorcov správania v sieti, ako sú skenovanie portov, útoky hrubou silou, tunelová komunikácia, slepá komunikácia atď.

ANALÝZA OPAKUJÚCEHO SA SPRÁVANIA

Táto metóda rozlišuje medzi nepredvídateľnými vzorcami ľudského správania a predvídateľnými vzorcami strojového správania. Táto schopnosť je založená na dlhodobom spracúvaní údajov uložených v databáze, čo umožňuje nástroju Mendel odhaliť komunikáciu infikovaných hostiteľov, ktorí boli napadnutí trójskymi koňmi pre vzdialený prístup (RAT), malvérom využívajúcim riadiace C&C servery, pokročilými pretrvávajúcimi hrozbami (APT) atď. Výhodou tohto prístupu je možnosť odhaliť komunikáciu malvéru prostredníctvom rôznych protokolov vrátane HTTP/S, DNS alebo ICMP.

VÝKONNOSTNÁ ANALÝZA

Moduly monitorovania výkonnosti siete a aplikácií analyzujú efektivitu prenosu údajov a porušenia SLA v prípade rôznych protokolov vrátane HTTP/S, MS-SQL alebo SIP.

ANALÝZA ZALOŽENÁ NA PRAVIDLÁCH

Udalosti sa reportujú na základe pravidiel definovaných používateľom, ako je prenos údajov, toky, priepustnosť paketov, prahové hodnoty podsietí, hostiteľov, služieb, povolené alebo zamietnuté komunikačné vektory (audit firewallu) atď.

Detekčné jadrá

SYSTÉM DETEKCIE VNIKNUTIA (INTRUSION DETECTION SYSTEM – IDS)

Kontroluje komunikáciu na úrovni paketov a vyhľadáva známe hrozby, ako sú trójske kone, malvér, exploity atď. Mendel má k dispozícii viac ako 85 000 pravidiel na detekciu hrozieb číhajúcich v sieti.

KORELAČNÉ JADRO

Dáva do vzájomného vzťahu viaceré udalosti, pričom upozorňuje na vážnejšie problémy zvýšením závažnosti udalosti. Predvolene sú v nástroji Mendel zahrnuté viaceré korelácie, napríklad šírenie malvéru, detekcia sietí Tor atď.

SPRACOVANIE PROTOKOLOV

Schopnosť spracovávať prijaté protokoly a generovať z nich bezpečnostné udalosti polopasívnym prístupom (protokoly prijaté nástrojom Mendel na zadanom porte).

OZNAČOVACIE JADRO

Rozšírená klasifikácia zariadení a ich úloh. Dynamický prehľad vďaka sledovaniu nových aktivít alebo zmien spôsobených zariadeniami komunikujúcimi v sieti. Úplne nové jadro, ktoré prináša manuálny alebo automatizovaný spôsob označovania hostiteľov alebo podsietí prostredníctvom systému pravidiel definovaných používateľom s ľahko zrozumiteľnou syntaxou.

INFORMÁCIE O HROZBÁCH

Využívané informačné kanály o hrozbách zahŕňajú databázy IP adries zaradených na blacklist a ich reputácie, a to z komerčných aj otvorených zdrojov (ProofPoint, SpamHouse, blocklist.de, abuse.ch atď.). Mendel dokáže využívať aj informačné kanály služby ESET Threat Intelligence na detekciu škodlivých domén podľa ich URL adries či detekciu súborov podľa ich hashov. Tieto informačné kanály sa dodávajú vo formáte STIX-TAXII.

Spracovanie a analýza komunikácie

HĹBKOVÁ KONTROLA PAKETOV

- Monitoruje akúkoľvek interakciu s internou sieťou alebo v rámci nej
- Umožňuje kontrolu komunikácie až do 100 Gbit/s
- Detekčné signatúry pre malvér, porušenia politík, útoky a iné aktivity
- Detekcia škodlivých súborov podľa hashu
- Komunikácia s hostiteľmi na blackliste
- Možnosť pridávať podpisy vytvorené používateľom

MONITOROVANIE VÝKONNOSTI

Analýza výkonnosti siete a aplikácií na základe tokov (NPM, APM):

- Informovanosť o aplikáciách
- Monitorovanie aktuálnej a priemernej šírky prenosového pásma
- Monitorovanie výkonnostných ukazovateľov, ako sú časy odozvy aplikácie, komunikačné oneskorenie, čas strávený interakciou používateľa s prostredím
- Detekcia na základe pravidiel (napr. SLA)
- Automatická detekcia anomálií

HISTORICKÉ METADÁTA A FORENZNÁ ANALÝZA

Protokol ASNM (Advanced Security Network Metrics) nástroja Mendel je zameraný na bezpečnosť a výkonnosť a slúži na pokročilý opis sieťovej komunikácie.

Ponúka tieto možnosti:

- Obojsmerný záznam toku (jeden tok obsahuje žiadosť aj odpoveď)
- Metadáta aplikačných protokolov pre FTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, SSL/TLS, Kerberos atď.
- Metadáta priemyselných protokolov pre Modbus, DNP3, IEC 60870-5-104, IEC 61850 (GOOSE, MMS, SV), ENIP/CIP, CC-link, GE-SRTP
- Údaje možno uchovávať mesiace alebo roky (v závislosti od kapacity úložiska)

ANALÝZA SPRÁVANIA SIETE

Analýza sieťovej komunikácie na základe toku s využitím strojového učenia bez učiteľa a niekoľkých detekčných techník (pozri vyššie).

Schopnosti detekcie:

- Aktivita malvéru – šírenie, sťahovanie, rozosielanie spamu atď.
- Aktivita útočníka – skenovanie, hrubá sila, zneužitie zraniteľnosti atď.
- Aktivita C&C – RAT, APT, AVT, boty, červy, rootkity atď.
- Exfiltrácia údajov

ZAZNAMENÁVANIE KOMUNIKÁCIE

- Manuálne zachytávanie paketov
- Na základe zdrojovej a cieľovej IP adresy, MAC adresy, protokolu, portu atď.

Hlavné výhody

SPRÁVA INCIDENTOV

- Možnosti správy incidentov vrátane označovania udalostí ako incidentov a sledovania reportov o procese vyšetrovania
- Jednoduché manažérske a analytické reporty za rôzne časové intervaly

DETAILNÝ PREHĽAD O SIETI

- Všetky podsiete, hostitelia, služby a toky s podrobnými informáciami
- Metadáta poskytujú dostatok informácií o správaní siete na účely forenzného vyšetrovania, dodržiavania predpisov atď.
- Tunelová komunikácia
- Dešifruje zašifrovanú komunikáciu pomocou dešifrovacieho kľúča
- Automatická identifikácia kritických zariadení v sieti, ako je služba Active Directory, e-mailový server atď.
- Historické údaje za niekoľko mesiacov sú indexované a rýchlo dostupné
- Výkonné vyhľadávanie zozbieraných údajov pomocou filtrovania

ANALÝZA ZRKADLENEJ KOMUNIKÁCIE

- Citlivejšia detekcia správania než NetFlow (a podobné protokoly)
- V porovnaní s protokolom NetFlow/IPFIX záznamy obsahujú aj parametre zabezpečenia a metriky výkonu

SPOĽAHLIVÁ DETEKCIA

- Zero-day a pokročilé hrozby (APT atď.)
- Trójske kone pre vzdialený prístup (RAT)
- Únik údajov (zneužitie DNS, SSH, HTTP(S), ICMP atď.)
- Tunelová komunikácia (DNS, SSH, HTTP(S), ICMP atď.)
- Anomálie v protokoloch
- Skenovanie portov
- Slovníkové útoky a útoky hrubou silou
- Krádež údajov a iné interné hrozby
- Porušenie interných bezpečnostných politík
- Zlá konfigurácia siete
- DoS, DDoS
- Automatizovaný zber dát (napr. e-shop)
- Analýza šifrovanej komunikácie (certifikáty SSL, odtlačky atď.)

NETFLOW

- Až do 50 Gbit pôvodnej komunikácie
- Až 1 000 externých zdrojov (prepínačov)
- Ukladanie údajov HTTP, TLS a DNS pomocou protokolu IPFix
- Extrakcia výkonnostných metrík
- Extrakcia parametrov, napr. prichádzajúce rozhranie
- Detegované IP adresy na blackliste
- Výkonnostné profily
- Podpora viacerých rozhraní zariadenia

INVENTÁR SIETE

- Zlúčenie prehľadu a vrstvy detekcie do jedného prehľadného zobrazenia
- Sieťová infraštruktúra s pridanou hodnotou v podobe podrobných informácií o podsieťach a hostiteľoch, s vypočítaným rizikom a premysleným prístupom k bezpečnosti
- Údaje prezentované v tabuľke s možnosťou filtrovania alebo v škálovateľnej grafickej podobe