GREYCORTEX Mendel Data Sheet

Mendel od společnosti GREYCORTEX, NDR řešení pro podniky, státní správu a kritickou infrastrukturu v oblasti síťové bezpečnosti nabízí hlubokou viditelnost v síti, pokročilou detekci a reakci na hrozby.

Mendel sleduje a analyzuje síťový provoz, pomáhá odhalovat známé i neznámé hrozby způsobené externím útočníkem i zaměstnanci, a to včetně úniků dat, provozních anomálií a dalších obtížně odhalitelných hrozeb. Díky zpracování zrcadleného provozu z páteřních přepínačů poskytuje Mendel hlubokou viditelnost pro celou monitorovanou síť. Nasazení během několika minut zaplní mezery po tradičních bezpečnostních nástrojích a zkrátí čas a ušetří zdroje potřebné k zajištění bezpečnosti a spolehlivosti síťových operací.

Metody detekce

Prediktivní analýza	Učí se a předvídá chování sítě pro všechny její podsítě, zařízení, uživatele a služby. Veškerý provoz, který není v souladu s trénovanými modely chování, je analyzován jako anomální (tedy například abnormální přenosy dat, objemy komunikace mezi koncovými zařízeními, přehledy komunikace přes jednotlivé porty, počty toků, délka komunikace, doba komunikace apod.). Naučené modely Mendel každou hodinu znovu upraví, a přizpůsobí se tak všem změnám.
Analýza změn na síti	Aktivně sleduje a zaznamenává přehled komunikujících služeb a hostitelů v síti. Pokud se ve sledovaném segmentu sítě objeví nový hostitel (například BYOD) nebo nová služba, je hlášena událost. Stejná metoda se používá, když služby nebo hostitelé přestanou komunikovat, změní své MAC adresy nebo když se změní názvy DNS. Dále Mendel sleduje komunikaci mezi povolenými a zakázanými službami na základě přednastavených politik.
Analýza toků	Detekuje známé nežádoucí vzorce chování v síti, jako jsou skenování portů, útoky hrubou silou, tunelovaná komunikace, slepá komunikace, atd.
Repetitivní analýza	Tato metoda rozlišuje mezi nepředvídatelnými vzorci lidského chování a předvídatelnými vzorci strojového chování. Je založena na dlouhodobém zpracování uložených dat v databázi, což umožňuje detekovat komunikaci infikovaných hostitelů, kteří byli napadeni technikami RAT, C&C malware, APT, apod. Tento přístup přináší schopnost detekovat malware komunikaci prostřednictvím více protokolů včetně HTTP/S, DNS nebo ICMP.
Analýza výkonu	Modul pro monitorování výkonu sítě a monitorování výkonu aplikací analyzuje efektivitu přenosu dat a porušení SLA pro různé protokoly včetně HTTP/S, MS-SQL nebo SIP.
Signaturní analýza	Události na základě systémových nebo uživatelsky definovaných pravidel, jako je přenos dat, toky, propustnost paketů, prahové hodnoty v podsítích, hostitelích, službách, povolených nebo zakázaných komunikačních vektorech (audit brány firewall) atd.

Detekční nástroje

Systém detekce narušení (IDS)	Kontroluje komunikaci na úrovni paketů, vyhledává známé hrozby, jako jsou trojský kůň, malware, exploity atd. Mendel využívá více než 85 000 pravidel pro detekci hrozeb v síti.
Korelace	Koreluje jednotlivé události a jejich spojením upozorňuje na závažnější problémy. Ve výchozím nastavení Mendel pokrývá korelace, jako je šíření malwaru, detekce sítí Tor apod.
Znalostní báze hrozeb	Informační kanály o hrozbách zahrnují databáze IP adres uvedné na blacklistech a jejich reputace. Mendel čerpá z komerčních i volně dostupných zdrojů (ProofPoint, SpamHouse, Blocklist.de, Abuse.ch atd.). Dále je jako zdroj dostupný ESET Threat Intelligence a MISP k detekci škodlivých domén podle URL a souborů (hash). Tyto zdroje jsou distribuovány ve formátu STIX-TAXII.
Tagování	Rozšířená klasifikace zařízení a jejich rolí. Dynamická viditelnost díky sledování nových aktivit nebo změn způsobených zařízeními komunikujícími ve vaší síti. Zcela nový nástroj, který přináší ruční nebo automatizovaný způsob označování hostitelů nebo podsítí prostřednictvím systému uživatelsky definovaných pravidel se snadno srozumitelnou syntaxí.
Zpracování logů	Schopnost zpracovávat přijaté logy a generovat z nich bezpečnostní události semi-pasivním přístupem (logy přijaté Mendelem na zadaný port).

GREYCORTEX

Zpracování a analýza toků

Analýza síťového chování

Analýza síťového provozu založená na tocích prostřednictvím „unsupervised“ strojového učení a několika dalších detekčních metod (viz výše).

Možnosti detekce:

- Aktivita malwaru – šíření, stahování, spamování atd.
- Aktivita útočníka – skenování, brute-force, exploitace atd.
- Aktivita C&C – RAT, APT, AVT, boti, červi, rootkity atd.
- Exfiltrace dat

Záznam přenášených dat

Zachycení paketů na základě definované podmínky (události) nebo nastaveného.

Dále je možné definovat zdrojovou a cílovou IP, MAC adresou, protokolem, portem atd.

Hloubková kontrola paketů

- Monitoruje jakoukoli interakci s vnitřní sítí nebo uvnitř vnitřní sítě
- Umožňuje kontrolovat provoz až do rychlosti 100 Gbit/s
- Detekční signatury pro malware, porušení zásad, útoky a další aktivity
- Detekce škodlivých souborů pomocí hashování
- Komunikace s hostiteli na blacklistu
- Možnost přidávat signatury (pravidla) vytvořené uživateli

Monitorování výkonu

Analýza výkonu sítě a aplikací založená na tocích (NPM, APM):

- Povědomí o aplikacích
- Monitorování aktuální a průměrné šířky pásma
- Monitorování metrik výkonu jako jsou doba odezvy aplikace, round-trip, user-experience
- Detekce založená na pravidlech (např. SLA)
- Automatická detekce založená na anomáliích

Historická metadata a forenzní analýza

Advanced Security Network Metrics (ASNM) je zaměřen na bezpečnost a výkon, a slouží pro širší popis síťového provozu.

Zahrnuje:

- Obousměrný záznam toku (jeden tok obsahuje request i response)
- Metadata aplikačních protokolů pro FTP, SSH, Telnet, SMTP, DNS, DHCP, HTTP, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, SSL/TLS, Kerberos atd.
- Metadata průmyslových protokolů pro BACnet, CC-link, COAP, DLMS/COSEM, DNP3, ENIP, ETHERCAT, GE-STRP, IEC-104, IEC61850 (GOOSE, SV, MMS), MODBUS, MQTT, OMRON FINS, OPC UA, Profinet IO DCE/RPC, PROFINET-DCP, Siemens S7
- Retence dat v rozsahu měsíců až několika let (v závislosti na kapacitě úložiště)

Hlavní výhody

Analýza zrcadleného provozu a PCAP záznamů

- Citlivější detekce chování než čisté NetFlow (a podobné protokoly)
- Ve srovnání s NetFlow/IPFIX jsou záznamy rozšířeny o bezpečnostní parametry a výkonové metriky.

Robustní detekce

- Zero-day a pokročilé hrozby (APT atd.)
- Vzdálený přístup prostřednictvím Trojského koně (RAT)
- Únik dat (zneužití DNS, SSH, HTTP(S), ICMP atd.)
- Tunelovaný provoz (DNS, SSH, HTTP (S), ICMP atd.)
- Anomálie na protokolech
- Skenování portů
- Slovníkové útoky a útoky hrubou silou
- Krádeže dat a další interní hrozby
- Porušení zásad interní bezpečnosti
- Chybné konfigurace sítě
- DoS, DDoS
- Automatizovaný sběr dat (například z e-shopů, apod.)
- Analýza šifrovaného provozu (certifikáty SSL, otisky prstů atd.)

Viditelnost sítě do detailu

- Všechny podsítě, hostitelé, služby a toky obsahují podrobné informace
- Metadata poskytují dostatečné informace o chování sítě pro forenzní vyšetřování, soulad s předpisy atd.
- Tunelovaný provoz
- Dešifrování šifrované komunikace (pomocí příslušného klíče)
- Automatická identifikace kritických zařízení v síti, jako je Active Directory, e-mailový server, SMB server atd.
- Historická data jsou indexována a tedy rychle dostupná pro zobrazení
- Široké možnosti filtrování nad uloženými daty (přitom uživatelsky přívětivé)

Správa incidentů

- Označení události jako incidentu a následné sledování procesu vyšetřování (včetně notifikací)
- Jednoduché manažerské a analytické výstupy (reporty) pro různé časové intervaly

GREYCORTEX

Datový výstup

Grafické uživatelské rozhraní (GUI)

- Webové uživatelské rozhraní (Firefox, Chrome, Opera, Edge)
- Snadno přizpůsobitelné dashboardy (panely)
- Manažerské a bezpečnostní panely pro stručný přehled
- Rychlé a široké možnosti filtrování
- Průvodce tvorbou IDS pravidel
- Personalizace vzhledu (motivu)
- Kontextová nápověda a obsáhlá uživatelská dokumentace

Reporty a notifikace

- Reporty generované na základě definovaných podmínek
- Přizpůsobitelný výstupní formát s možností vložení odkazu přímo do GUI
- Formáty vhodné pro koncového uživatele: e-mail (HTML) a PDF

Integrace

- SIEM: formáty CEF (Common Event Format), CEF Standard, LEEF (Long Extended Event Format), Syslog nebo reportovací protokol IDEA
- Integrační balíček pro platformu XSOAR
- Export toků ve formátu IPFIX
- Active Directory a Cisco ISE pro doplnění identity uživatele
- E-mailový server
- Firewall (MikroTik, Juniper, FortiGate, Palo Alto, Checkpoint atd.)
- Přizpůsobitelná Integrace s další infrastrukturou možná prostřednictvím RestAPI
- Přizpůsobitelný výstupní formát

Datová integrace

Síťová data

- Zrcadlený provoz (TAP, SPAN nebo jiný typ zrcadleného datového portu)
- Podpora linkové vrstvy
- Podpora síťové vrstvy včetně protokolů IPv6
- Podpora transportní vrstvy
- Podpora aplikační vrstvy
- Z jiných zařízení Mendel (senzor nebo kolektor)
- Protokoly založené na Flow (NetFlow rodina, IPFIX)

Znalostní báze hrozeb

- IDS signatury z Proofpoint a dalších zdrojů
- Ostatní relevantní databáze (IP reputace, doménová reputace, GEO IP, WHOIS, ...)
- Databáze škodlivých souborů (např. ESET Threat Intelligence)
- Definice událostí podle Mitre ATT&CK Enterprise a Mitre ATT&CK ICS frameworků

Znalost sítě

- Definic epolitik podle segmentů/podsítí, které sdílejí stejné vzorce chování, např. management, obchod, servery, WiFi, VoIP, tiskárny, DMZ atd.
- Spojení IP s názvem hostitele (pomocí DNS záznamů)

Znalost uživatelů

- Spojení IP s doménou (prostřednictvím logů z doménových řadičů, LDAP)

Škálovatelnost nasazení

Škálovatelnost nasazení se může lišit dle konkrétních podmínek a kombinací v cílové infrastruktuře.

Senzor

- Monitorování sítě s propustností až 100 Gbps
- Rozhraní s možností až 8× 1GE rozhraní nebo 4× 10GE rozhraní nebo 2× 100GE
- V režimu virtualizace nebo Cloud nasazení zpracování až 4 Gbps

Kolektor

- Spojení více jak 40 senzorů pod jedním kolektorem
- Až 50 000 monitorovaných síťových uzlů na jeden kolektor
- Historická data dostupná od měsíců až po několik let
- Nasazení ve virtualizovaném prostředí (vč. Cloudu) se zpracováním až 20 připojených senzorů
- Úložiště s více diskovými oddíly s podporou rychlých disků (NVMe, SSD, SAS)

All-in-One

- Jedno zařízení obsahující zároveň senzor i kolektor
- Monitorování sítě s propustností až 100 Gbps
- Rozhraní s možností až 8× 1GE rozhraní nebo 4× 10GE rozhraní nebo 2× 100GE
- Až 20 připojených dalších senzorů na jedno All-in-One zařízení
- Až 50 000 monitorovaných uzlů na jedno All-in-One zařízení
- Úložiště s více diskovými oddíly s podporou rychlých disků (NVMe, SSD, SAS

Centrální správce událostí

- Spojení až 20 kolektorů do jednoho centrálního místa
- Přehled všech událostí na jednom místě z celé připojené infrastruktury

GREYCORTEX