GREYCORTEX Mendel Data Sheet

NDR

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

ZDROJE DAT

- Zrcadlený síťový provoz
- NetFlow/IPFIX
- Síťové a aplikační protokoly
- Zaznamenaný síťový provoz (PCAP)

DETAILNÍ VIDITELNOST SÍTĚ

- Všechny podsítě, hosté, služby a toky obohacené o podrobné informace
- Metadata poskytují bohaté informace o chování sítě pro účely forenzního vyšetřování, zjištění souladu 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

VÝKONNÁ DETEKCE

na základě procesů strojového učení, matematických modelů, s eliminací falešně pozitivních výsledků

PREDIKTIVNÍ ANALÝZA

- Volumetrické anomálie
- DDoS útoky

Využívá pokročilé algoritmy umělé inteligence a strojového učení k předvídání a identifikaci potenciálních bezpečnostních hrozeb dříve, než se projeví jako plnohodnotný útok.

ANALÝZA ZMĚN NA SÍTI

- Nová zařízení, služby a komunikační vektory
- Nové administrátorské přístupy

Proces systematického zkoumání a mapování síťového prostředí s cílem identifikovat aktiva, zranitelná místa a potenciální místa kompromitace.

ANALÝZA TOKŮ

- Skeny
- Útoky hrubou silou
- Enumerace

Investigace a interpretace toků síťového provozu s cílem zajistit přehled o komunikačních vzorcích, chování a potenciálních bezpečnostních hrozbách.

REPETITIVNÍ ANALÝZA

- Command & Conquer
- Útoky hrubou silou

Identifikace a analýza opakujících se vzorců nebo chování v síťovém provozu s cílem odhalit potenciální bezpečnostní hrozby nebo anomálie.

ANALÝZA VÝKONU

- Problémy s výkonem sítě: vysoká doba odezvy, slow round trip time

Vyhodnocování a optimalizace provozní efektivity, spolehlivosti a škálovatelnosti bezpečnostních systémů a síťové infrastruktury prostřednictvím průběžného sledování výkonnostních ukazatelů.

ANALÝZA LOGŮ

- Nový firmware, noví uživatelé
- Změny v registrech a nastaveních

Shromažďování, analýza a rozbor dat protokolů generovaných různými síťovými zařízeními, systémy a aplikacemi za účelem identifikace bezpečnostních incidentů, anomálií a provozních problémů.

REAKCE

- Centralizovaná platforma pro sledování, dokumentování a hlášení bezpečnostních incidentů.
- Systém pluginů pro univerzální způsob interakce s firewally, NAC atd.
- Rozsáhlé možnosti exportu dat pro sdílení dat s jinými bezpečnostními nástroji

ANALÝZA NA ZÁKLADĚ PRAVIDEL

- Detekce známého malwaru a exploitů
- Porušení bezpečnostních zásad
- Security policies violations

Metoda identifikace a vyhodnocování bezpečnostních hrozeb na základě předem definovaných pravidel nebo kritérií pro detekci a reakci v reálném čase.

KLÍČOVÉ SCHOPNOSTI

Analýza chování sítě

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

Detekční schopnosti:

- 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

Hloubková kontrola packetů

- Monitoruje jakoukoli interakci s interní sítí nebo uvnitř ní
- Umožňuje kontrolovat provoz až do rychlosti 100 Gbit/s
- Detekční signatury pro malware, porušení politik, útoky a další závadné aktivity
- Detekce škodlivých souborů pomocí hashování
- Přehled komunikace s hosty na blacklistu
- Možnost přidávat signatury (pravidla) vytvořené uživateli

Network Inventory

- Sloučení vrstev Viditelnost a Detekce do jednoho společného pohledu
- Zobrazení síťové infrastruktury z pohledu podsítí a zařízení, doplněná o rizika a další bezpečnostní pohledy
- Přehledná interpretace dat formou srozumitelných tabulek a grafických přehledů

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 (například SLA)
- Automatická detekce založená na anomáliích

Historická metadata a forenzní analýza

Proprietární protokol Advanced Security Network Metrics (ASNM) je zaměřený 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/S, NTP, SMB, SNMP, LDAP, NFS, MS-SQL, SIP, SSL/TLS, Kerberos atd.
- Retence dat v rozsahu měsíců až několika let (v závislosti na kapacitě úložiště)

Kategorizace zařízení

- Rozšířená klasifikace zařízení a jejich rolí prostřednictvím systémových či vlastních tagů
- Dynamická viditelnost díky sledování nových aktivit nebo změn způsobených zařízeními komunikujícími ve vaší síti
- Ruční nebo automatizovaný způsob označování hostitelů nebo podsítí podle pravidel vytvořených uživatelem pomocí snadno pochopitelného průvodce

Záznam a přehrávání provozu

- Zachycení paketů na základě definované podmínky (události) nebo podle dalších pravidel na základě zdrojové a cílové IP, MAC, protokolu, portu atd.
- Možnost přehrávat a analyzovat PCAPy zaznamenané samotným nástrojem Mendel nebo zpracovat přenosy zachycené jinými nástroji

OT schopnosti

- Detekce, parsování a hlášení událostí včetně bohatých metadat pro průmyslové protokoly 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, SNMP
- Specifické detekční OT signatury definované GREYCORTEX
- Metriky OT aplikací
- Detekce průmyslových zařízení (Asset discovery)
- Společná prezentace dat podle Purdue a MITRE ATT&CK

VSTUPY

Komplexní přístup k analytickému zpracování dat z mnoha různých zdrojů pro zajištění síťové bezpečnosti, a to včetně různých vrstev modelu OSI, využití znalostní báze hrozeb, funkcí dohledu chování jednotlivých sítí a jejich uživatelů pro účinné prosazování nastavených interních politik a zmírňování či eliminaci hrozeb.

Síťová data

- Zrcadlený provoz (TAP, SPAN, RSPAN, ERSPAN nebo jiný typ zrcadleného provozu)
- Podpora linkové vrstvy
- Podpora síťové vrstvy včetně protokolů IPv6
- Dekapsulace tunelovaného provozu
- Podpora transportní vrstvy
- Podpora aplikační vrstvy
- Protokoly založené na Flow (NetFlow family, IPFIX, sFLOW, JFlow, NetStream a protokoly toku VPC)
- Z jiných zařízení Mendel (senzor, mikrosenzor nebo kolektor)

Znalostní báze hrozeb

- Soubor detekčních pravidel Proofpoint Emerging Threats a interní výzkum GREYCORTEX
- Další databáze informací o hrozbách IP adres, doménových reputací a škodlivých souborů
- Možnost integrace vlastních informačních kanálů TI (včetně národních platforem MISP)
- Definice události podle MITRE ATT&CK Enterprise a Mitre ATT&CK ICS

Znalost sítě

- Definice politik podle segmentů/podsítí, které sdílejí stejné vzorce chování, například management, obchod, servery, WiFi, VoIP, tiskárny, DMZ atd.
- Spojení IP s doménou (pomocí DNS záznamů)

Znalost uživatelů

- Spojení IP s názvem hosta (prostřednictvím logů z doménových řadičů, AD, LDAP, CISCO ISE a všechny poskytnuté protokoly s těmito informacemi v rámci sledované sítě od různých služeb)

VÝSTUPY

Systém poskytuje komplexní sadu výstupů a integrací pro efektivní monitorování a správu zabezpečení sítě a zajišťuje účinné monitorování, analýzu a reakci na bezpečnostní incidenty.

Grafické uživatelské rozhraní (GUI)

- Webové uživatelské rozhraní (Firefox, Chrome, Opera, Edge)
- Hlavní interaktivní pohled založený na znalostech GREYCORTEX a frameworku MITRE ATT&CK®.
- Rozsáhlé snadno přizpůsobitelné dashboardy
- Manažerské a bezpečnostní dashboardy pro zjednodušený přehled
- Operativní a široké možnosti filtrování
- Průvodce tvorbou vlastních IDS pravidel
- Dva motivy designu (světlý a tmavý)
- Kontextová nápověda a obsáhlá uživatelská dokumentace

Reporty a notifikace

- Reporty generované na základě definovaných podmínek
- Bohatý a přizpůsobitelný výstupní formát s možností přidání přímého odkazu do GUI
- Formáty vhodné pro koncového uživatele: e-mail (HTML) a PDF

Integrace

- SIEM – formáty CEF, LEEF, Syslog nebo API
- SOAR – přizpůsobitelná integrace založená na exportu událostí a API s integračním balíčkem pro Palo Alto XSOAR
- XDR – přizpůsobitelná integrace s platformami EDR na základě rozhraní API nebo podle specifik dodavatele
- IPFIX – export toků ve formátu IPFIX
- IDENTITA – Active Directory, Cisco ISE a běžné externí protokoly pro doplnění identity uživatele
- FIREWALL/NAC – MikroTik, Juniper, FortiGate, Palo Alto, Checkpoint atd.
- OUTPUT – Přizpůsobitelné datové výstupy
- API – Obecné rozhraní RESTful API pro integraci s další infrastrukturou

NASAZENÍ

Škálovatelnost nasazení se liší podle konkrétních podmínek a kombinací v dané infrastruktuře.

Senzor

- Monitorování sítě s propustností až 100 Gbps
- Až 20 monitorovacích rozhraní na každém HW zařízení s libovolnou kombinací 1GbE, 10GbE, 25GbE nebo s HW akcelerovanými kartami FPGA až 8× 25/10GbE nebo 4×100/40GbE
- V režimu virtualizace nebo Cloud nasazení zpracování až 10 Gbps
- Volitelně malý HW mikrosenzor s monitorovacími porty až 3× 1GbE

Kolektor

- Až 100 senzorů pod jedním kolektorem (na základě celkové zpracovávané kapacity)
- Až 150 000 monitorovaných síťových uzlů na jeden kolektor
- Uchovávání historických dat je omezeno pouze velikostí dostupného (navrženého) datového úložiště
- Nasazení ve virtualizovaném prostředí (včetně Cloudu) se zpracováním až 20 připojených senzorů
- Úložiště s více diskovými oddíly s podporou rychlých disků (NVMe, SSD, SAS)
- Možnost online a offline aktualizace samotného systému nebo připojených senzorů

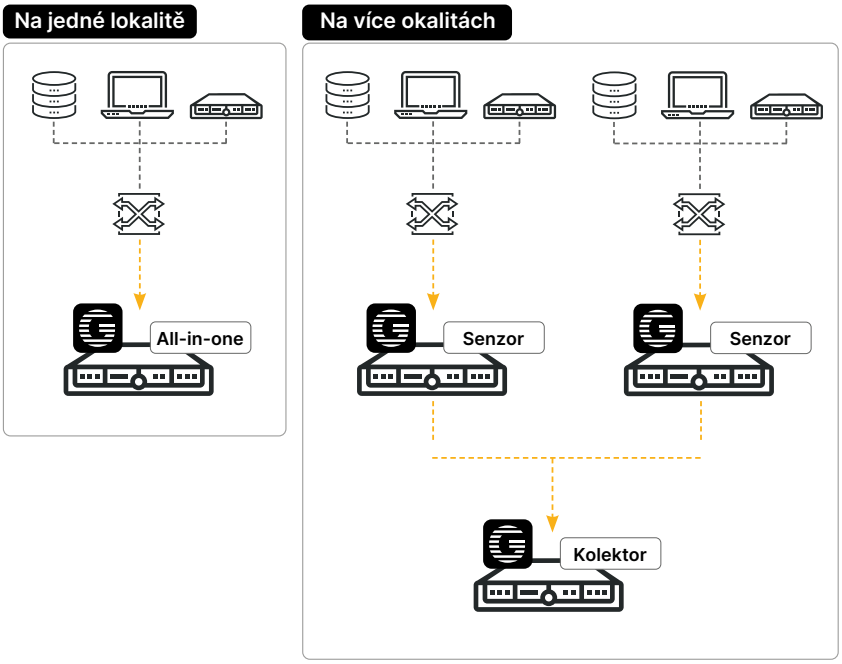
All-in-One

- Jedno zařízení obsahující zároveň senzor i kolektor
- Monitorování sítě s propustností až 50 Gbps
- Až 20 monitorovacích rozhraní na každém HW zařízení s libovolnou kombinací 1GbE, 10GbE, 25GbE nebo s HW akcelerovanými kartami FPGA až 8× 25/10GbE nebo 4×100/40GbE
- 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)
- Možnost online a offline aktualizace samotného systému nebo připojených senzorů

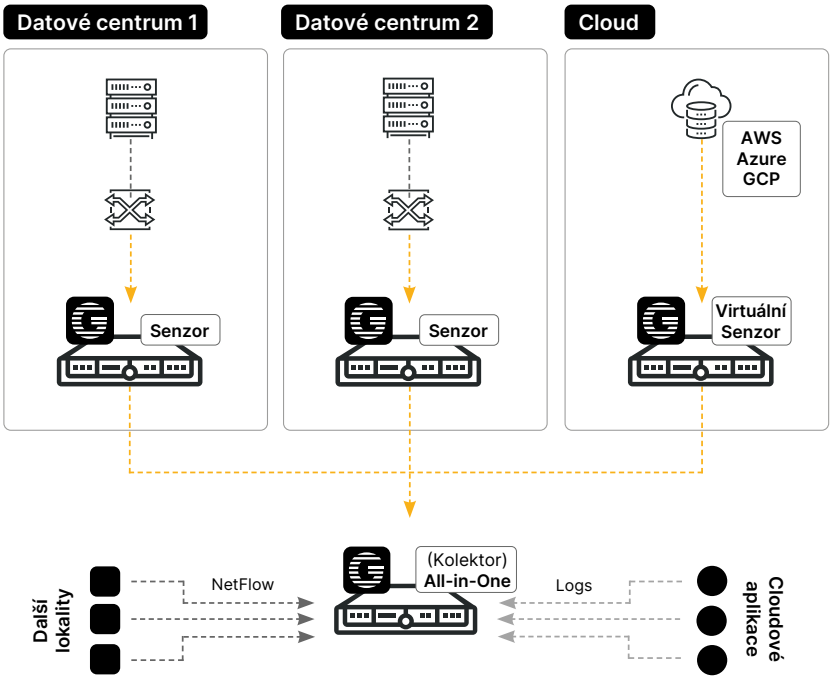
Centrální správa událostí

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

Nasazení



Nasazení na více lokalitách



Vyzkoušejte GREYCORTEX Mendel

Proof of Concept (PoC)
Pro vyzkoušení GREYCORTEX Mendel vám nabízíme měsíční bezpečnostní audit sítě.

Purkyňova 127, 612 00 Brno, Czech Republic, +420 511 205 216, info@greycortex.com

www.greycortex.com