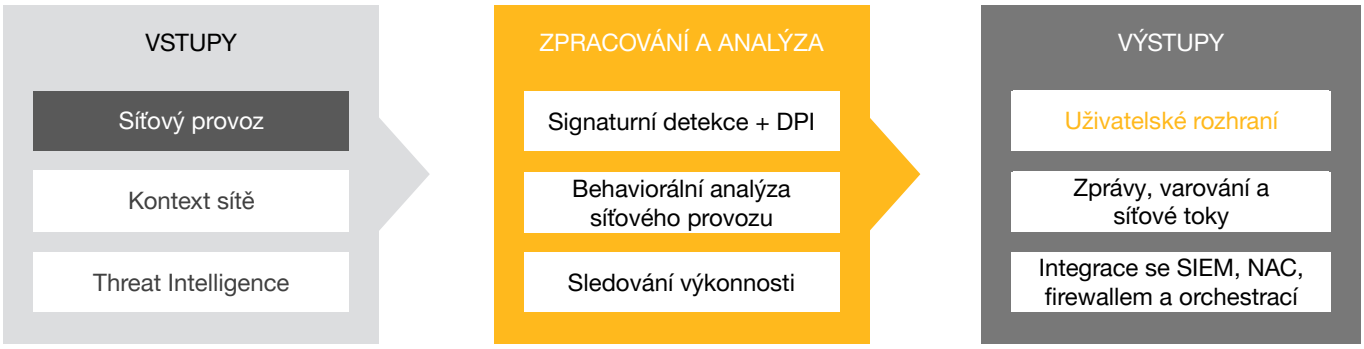
GREYCORTEX MENDEL

PRODUKTOVÝ LIST

GREYCORTEX MENDEL je pokročilý nástroj pro analýzu síťového provozu, sledování výkonu, detekci hrozeb a hlubokou viditelnost do sítě pro podniky, úřady a kritickou infrastrukturu. K analýze a sledování síťového provozu MENDEL využívá umělou inteligenci a strojové učení. To umožňuje detekci nových a neznámých útoků zevnitř organizace i zvnějšku, úniků dat, provozních anomálií a jiných pokročilých hrozeb neviditelných pro jiné bezpečnostní technologie. MENDEL je okamžitě připraven zaplnit mezery, které nepokrývají tradiční bezpečnostní nástroje, a tím snižuje čas i množství zdrojů potřebných k zajištění bezpečností a spolehlivosti firemního IT.



Detekční metody

MENDEL nepřetržitě monitoruje síťový provoz a využívá řadu pokročilých metod detekce škodlivého, anomálního a podezřelého chování:

Prediktivní analýza	Na základě dříve naučeného chování sítě, každé podsítě, zařízení a služby na každém zařízení, je GREYCORTEX MENDEL schopen předpovídat očekávané komunikační chování. Síťový provoz, který není v souladu s predikovaným chováním, je hlášen jako anomální. Příklady anomálií: přenos dat, počet komunikačních partnerů, počet komunikačních portů, počet síťových toků atd.
Analýza změn na síti	MENDEL udržuje aktuální seznam aktivních síťových služeb a zařízení. Pokud se na sledovaném segmentu sítě objeví nové zařízení (například zařízení dle politiky BYOD) nebo služba, nahlašuje se událost. Stejná metoda se používá, když služby nebo zařízení přestanou komunikovat, mění MAC adresy nebo změní DNS jméno. Tato metoda také oznamuje komunikaci prostřednictvím povolených a zakázaných služeb na základě přednastavených politik.
Analýza síťových toků	Detekce známých a nežádoucích chování v síti, jako jsou skenování portů, slovníkové útoky a útoky hrubou silou, vysoký počet síťových toků atd.
Repetitivní analýza	Tato metoda rozlišuje lidské chování, které není předvídatelné, a strojové chování, které lze předvídat. Tato schopnost je založena na dlouhodobém zpracování uložených dat, což umožňuje detekovat komunikaci infikovaných zařízení, která byla napadena RAT, malwarem, využívajícím C&C, APT atd. Dodatečným přínosem této analýzy je schopnost detekovat malwarovou komunikaci prostřednictvím různých protokolů včetně HTTP/S, DNS nebo ICMP.
Analýza výkonnosti	Sledování výkonnosti sítě a sledování výkonnosti aplikací analyzují efektivitu přenosu dat pro různé protokoly včetně protokolu HTTP/S, MS-SQL nebo SIP. Výkonnostní metriky jsou také modelovány, takže pokud nějaký server začne mít problém s výkonem, systém upozorní na anomálii, např. na dobu odezvy aplikací, aniž by bylo nutné nastavovat prahové hodnoty manuálně. Výkonnostní metriky se učí automaticky.
Analýza na základě pravidel	Události jsou hlášeny na základě pravidel definovaných uživatelem, jako jsou přenos dat, počet toků, paketů, prahové hodnoty pro podsítě, zařízení, služby, povolené nebo nepolovelné komunikační vektory (audit firewallu).
Analýza na základě signatur	Události jsou hlášeny na základě detekce běžných nebo předvídatelných hrozeb, škodlivého softwaru a útoků v několika kategoriích, jako jsou C&C, P2P, Malware, trojské koně, Chat, Web, zranitelnosti, TOR, skenování, porušení politik atd.

Zpracování a analýza provozu

Behaviorální analýza síťového provozu

Analýza síťového provozu na základě toků, strojového učení, inteligentní eliminace falešných poplachů a několik detekčních kategorii (viz výše).

Detekční schopnosti:

- Malwarové aktivity – šíření, stahování, spamování atd.
- Útočnické aktivity – skenování, útoky hrubou sílou, zneužívání zranitelností atd.
- C&C aktivity – RAT, APT, AVT, bot, worm, rootkit atd.
- Exfiltrace dat

Hloubková inspekce paketů (DPI)

Volitelné nahrávání veškerého provozu dle definovaného filtru na základě zdrojové a cílové adresy IP, MAC, podsítě, protokolu, portu, rodiny IP (IPv4, IPv6). Toky jsou obohaceny aplikačními L7 metadaty pomocí DPI.

Detekce na základě signatur

Detekce průniků na základě signatur:

- Interní monitoring sítě
- Vícevláknové zpracování
- Několik zdrojů komerčních signatur
- Detekce známých hrozeb, útoků a jiných škodlivých aktivit
- Profilování pravidel a vlastní pravidla výkonnostních odchylek

Sledování výkonnosti

Analýza výkonnosti sítě a aplikací na základe toků a paketů (NPM, APM):

- Detekce aplikací
- Sledování aktuální a průměrné šířky pásma, doby odezvy, round trip time, odezva z pohledu uživatele, doby odezvy serveru atd.
- Automatická detekce výkonnnostních anomálií

Historická metadata

Protokol ASNM (Advanced Security Network Metrics) je protokol zaměřený na bezpečnost a výkon, který poskytuje mnohem hlubší analýzu provozu než protokol NetFlow.

ASNM zahrnuje:

- Obousměrné zaznamenávání toků (požadavek, odpověď) a deduplikace toků
- Metadata aplikačních protokolů – HTTP/S, SSL, TLS, SMB, SMB2, SMTP, FTP, SSH, DNS, XMPP, SIP, SSH, MS-SQL, DHCP, Modbus, DNP3 atd.
- Kompletní záznamy ASNM obsahují více než 900 parametrů
- Data mohou být uložena po dobu několika měsíců až několika let (v závislosti na kapacitě uložiště)

Hlavní výhody

Efektivní a výkonný

- Citlivější a spolehlivější
- Snižuje nároky a náklady na provoz a integraci

Mnohem víc než NetFlow

- Citlivější behaviorální detekce než NetFlow (a podobné protokoly)
- Záznamy NetFlow / IPFIX jsou obohaceny o bezpečnostní parametry a analýzu výkonnosti
- Detekce pomocí paketů zlepšuje detekci pomocí toků (jak pro bezpečnost, tak pro sledování výkonu)

Robustní detekce

- Zero day a pokročilé útoky (APT atd.)
- Remote Access Trojans (RATs)
- Únik dat (zneužité DNS, SSH, HTTP/S, ICMP atd.)
- Tunelovaný provoz (DNS, SSH, HTTP/S, ICMP atd.)
- Anomálie na úrovni protokolů
- Skenování portů
- Slovníkové útoky a útoky hrubou silou
- Příprava na vnitřní krádež dat a další vnitřní problémy, jako je porušení pravidel vnitřní bezpečnosti
- Nesprávná konfigurace sítě
- DoS, DDoS
- Automatický sběr dat (např. eshop)

Detailní viditelnost do sítě

- Kompletní informace o podsítích, zařízeních, službách, komunikačních partnerech a tocích
- Metadata poskytují dostatečné informace o chování sítě pro forenzní vyšetřování, dodržování politik atd.
- Historická data (měsíce až roky) jsou indexovaná a rychle dostupná

Hodnocení rizika

- Robustní schopnosti hodnocení rizika

Reportování

- Široce přizpůsobitelné reporty (včetně granularity reportů, upozornění atd.)
- Intuitivní webové grafické rozhraní
- Správa incidentů
- SIEM integrace přes syslog, CEF a LEEF, vč. toků v IPFIX
- Integrace s firewallem
- Orchestrační nástroje a další nástroje integrace

Výstupy

Grafické uživatelské rozhraní	Webové uživatelské rozhraní (IE, Firefox, Chrome, Opera, Safari, Edge atd.) – Zcela granulární přístupová práva s podporou multi-tenancy prostředí – Snadno přizpůsobitelné dashboardy – Neomezené filtrování a třídění
Reportování a varování	– Podmíněné reportování (varování) – Správa incidentů – Přizpůsobitelný výstupní formát – Čitelné formáty jako email (html), pdf, docx, vlastní odkazy do GUI
Integrace	– SIEM: Na základě formátu CEF (Common Event Format), LEEF (Log event extended format) nebo protokolu IDEA – Přizpůsobitelný výstupní formát – Export toků do IPFIX formátu s možností filtrování – Integrace s orchestračními nástroji a další infrastrukturou

Vstupy

Síťová data	– Zrcadlený síťový provoz (TAP, SPAN, ...) – Podpora IP vrstvy: vrstva L2 až L4 TCP/IP protokolu, včetně IPv6 protokolů – Protokoly založené na síťových tocích (rodina protokolů NetFlow, IPFIX)
Threat Intelligence	– Různé zdroje komerčních IDS signatur (Proofpoint ETPro) – Jiné databáze (IP reputace, reputace domén, GEO IP, WHOIS atd.)
Síťový pohled	– Definice funkčních segmentů sítě / podsítí (které sdílejí stejné vzory chování sítě, např. management, sales, servers, WiFi, VoIP, printers, DMZ atd.) – Překlad IP adres na názvy zařízení (pomocí záznamů DNS a DHCP)
Uživatelské identity	– Překlad IP adres na jména uživatelů (pomocí logů doménového řadiče, LDAP)

Appliance		Síťová propustnost Gbps							
		0.2	0.5	1	2	4	10	20	40
HW	All-in-One (Sensor + Collector)	✓	✓	✓	✓	✓	✓	✓	✓
	Collector				✓	✓	✓	✓	✓
	Sensor	✓	✓	✓	✓	✓	✓	✓	✓
VA	All-in-One (Sensor + Collector)	✓	✓	✓					
	Collector			✓	✓	✓	✓	✓	✓
	Sensor	✓	✓	✓					
	Central Event Manager	Propojení až 50 kolektorů nebo all-in-one (do 2Tbps)							

Prémiové služby	Vzdálená administrace	Pravidelné Threat Intelligence reporty	Okamžitý bezpečnostní report	Bezpečnostní poradenství	24x7 Prémiová podpora
MENDEL	o	o	o	o	o
MENDEL SaaS	✓	o	o	o	o

✓ standardní o volitelný

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

18-04/v1.42