GreyCortex Mendel – bezpečnostní monitoring a analýza síťového provozu

Šikovný bezpečnostní produkt, který nabízí širokou škálu zajímavých možností.

GreyCortex Mendel je řešení pro detekci, sledování a analýzu pokročilých bezpečnostních událostí v síťovém provozu. Toto řešení je založeno na kombinaci několika typů detekčních technologií:

- systém detekce průniku (Intrusion Detection System – IDS), včetně hloubkové inspekce paketů (Deep Packet Inspection – DPI
- systém detekce anomálií a analýzy chování sítě (Network Behavior Analysis – NBA); analýza je zde založena na principech umělé inteligence
- monitorování výkonu sítě a aplikací (Network Performance Monitoring – NPM a Application Performance monitoring – APM)
- nástroj pro korelaci událostí a posuzování rizik

Při návrhu produktu byl důraz kladen na vlastní pokročilé síťové metriky (Advanced Security Network Metrics – ASNM), dolování dat velkého rozsahu na bázi umělé inteligence a unikátní specializované algoritmy zajišťující detekci celé škály hrozeb a anomálií. Okamžité výstupy lze získat pomocí intuitivního webového uživatelského rozhraní a uživatelem definovaných reportů. GreyCortex ale přináší celou řadu dalších zajímavých možností, např. pro forensní účely poskytuje komplexní i detailní přehled o historii síťového provozu a o chování uživatelů, stanic v síti, aplikací a služeb. Produkt, původně TrustPort Threat Intelligence, nyní vyvíjí a podporuje nově formovaná společnost GreyCortex, do níž investoval fond Y Soft Ventures.

Zdroje dat

Hlavním vstupem je síťový tok dat ze zrcadleného portu na páteřním přepínači nebo z odboček typu TAP. Detektory NBA jsou schopny akceptovat sumarizovaná data ve formátu vlastních metrik ASNM, nebo dle standardů NetFlow v5/9, IPFIX pro IPv4 a IPv6. Kromě síťového provozu je produkt schopen zjišťovat kontext identity pomocí firemní LDAP anebo služeb Active Directory. Tyto technologie mohou být navíc použity pro správu uživatelů a jejich autentizaci.

Z externích zdrojů jsou získávána data detekčních signatur, které obsahují více než 30 000 pravidel. Dále jsou získávány blacklisty IP adres a jejich reputace (důvěryhodnost). Tyto seznamy jsou průběžně aktualizovány na hodinové nebo denní bázi. Nástroj tímto získává informace o všeobecně známém malwaru a o C&C (Command and Control) serverech útočníků, zdrojích útoků typu DDoS (Distributed Denial of Service) a známých botnetech. Dále je zde využíván seznam známých zdrojů

spamu, informace o sítích Tor[1] a o proxy serverech společně s informacemi o vlastnictví a geografické poloze komunikujících hostů a domén.

Protokol ASNM

Použitý protokol ASNM slouží pro sledování více než 70 atributů každého jednotlivého toku v síti. Pro každý tok sítě, je zde generována informace o zdroji a cíli, trvání, velikosti datové části, vedeny různé čítače paketů a rovněž zjišťovány spektrální a výkonnostní informace, jako je ART (Application Response Time), RTT (Round trip Time), Jitter a další.

Funkce pro detekci anomálního a potencionálně nežádoucího chování fungují obdobně jako u protokolu NetFlow, díky ASNM jsou však mnohem detailnější a tudíž i efektivnější. Další rozdíl spočívá ve schopnosti identifikovat konzistentní obousměrné toky v síti. Pro detekci aplikací je použit vlastní mechanismus rozpoznání aplikačních protokolů podobný standardu NBAR (Network-Based Application Recognition) používaného v zařízeních Cisco; mechanismus dokáže rozpoznat stovky protokolů. Technika DPI umožňuje extrahovat metadata pro téměř 30 aplikačních protokolů, a to i v rámci tunelového provozu.

Detekční mechanizmy

Pro detekci incidentů jsou použity dvě metody detekce na základě známých signatur (IDS) a detekce anomálií (NBA) založená na strojovém učení a umělé inteligenci. Celý mechanizmus učení spočívá v detailním modelování celé sítě v několika úrovních od modelů celé sítě až po modely jednotlivých služeb konkrétních hostů a zařízení.

Aplikace se dlouhodobě učí rozlišovat charakteristiky anomálních toků od normálních na základě pravděpodobnostních a statistických modelů, a to i bez nutnosti dekódování nebo dešifrování dat. Po instalaci do sítě je vždy nutné nechat aplikaci natrénovat se novému prostředí alespoň v jednotkách hodin. Plné znalosti dosáhne zhruba po jednom týdnu provozu.

Na protokolu ASNM jsou založeny následující algoritmy strojového učení:

- výběr relevantních individuálních metrik
- Bayesova analýza vycházející ze stanovených pravděpodobností událostí
- pravděpodobnostní modely typu GMM/EM (Gaussian Mixture Models/ Expectation-Maximization)

Pravděpodobnostní (Bayesovské) modelování poskytuje téměř 1000 parametrů rozdělených pro každý tok hostitele v síti či podsíti a jeho služby jak poskytované lokálně, tak těch, ke kterým se připojuje vzdáleně. Samostatný model je vytvořen pro každou službu hostitele, síťové zařízení, služby agregované na síti, masku podsítě, stát a ASN (Autonomous System Number).

Výstupy

GreyCortex Mendel poskytuje možnost vytvořené události exportovat v různých formátech a odesílat je prostřednictvím e-mailu nebo do vzdálených serverů SIEM (Security Information and Event Management) pro archivaci nebo další zpracování. Tato funkčnost umožňuje generovat výstrahy na základě stanovených podmínek a oznámeních o zjištěných anomáliích. Tímto způsobem lze vytvářet uživatelské sestavy, které obsahují textové nebo grafické znázornění detekovaných událostí, výkonu sítě nebo aplikací či jiných údajů v systému. Zprávy mohou obsahovat řadu přizpůsobitelných prvků včetně tabulek a různých grafů. Zprávy mohou být exportovány do standardních formátů dokumentů, jako je DOCX nebo PDF.

E-mailový systém podporuje připojení ke standardním e-mailovým serverům pomocí protokolu SMTP a šifrovanou komunikaci na bázi PGP (Pretty Good Privacy). Exporty dat lze provádět v předem definovaných intervalech nebo při detekci zvláště významné události. Nástroj rovněž podporuje export do systémů SIEM používajících Syslog, formát CEF (Common Event Format) nebo IDEA (Intrusion Detection Extensible Alert). Tyto zprávy mohou být předem konfigurovány a filtrovány podle různých potřeb systémové integrace.

Detekovat lze:

- trojské koně typu RAT (Remote Access Trojan) včetně aktivit systémů C&C
- slabiny typu Zero-day a exploitace služeb
- malware na mobilních a vestavěných zařízení
- dlouhodobé útoky APT (Advanced Persistent Threats)
- únik dat za pomoci DNS, SSH, HTTP(S) atd.
- tunelovaný provoz

[3] The Onion Routing - zajišťuje soukromí uživatele při práci na Internetu.

- protokolové anomálie svědčící o dlouhodobém skenování portů a dalších útočníkových aktivitách
- útoky typu maškaráda (útočník se vydává za někoho jiného), slovníkové útoky a útoky hrubou silou
- detekce spamu
- přípravu na krádež dat a exfiltraci (např. od zaměstnanců)
- automatizované sklízení dat
- krádeže dat (např. z webových aplikací)
- phishingové útoky
- nedodržení interních bezpečnostních pravidel a politik
- chybné nastavení sítě
- výkonnostní problémy sítě a aplikací
- útoky typu DoS a DDoS
- nová či cizí zařízení, např. typu BYOD (Bring Your Own Device)

Pro detekci širokého spektra hrozeb a aktivit slouží techniky fůze dat a korelace, které analyzují nejzajímavější informace získané o dané síti z různých detekčních mechanismů. Umožňuje zjišťovat korelace událostí, eliminovat falešná poplachy (false positives) a provádět odhady rizik. Zde je systém kompatibilní s takovými systémy pro kategorizaci rizik, jako jsou skórovací systém CVSS (Common Vulnerability Scoring System) nebo rámec NIST Critical Infrastructure Cybersecurity Framework [1] a další.

Průběh instalace

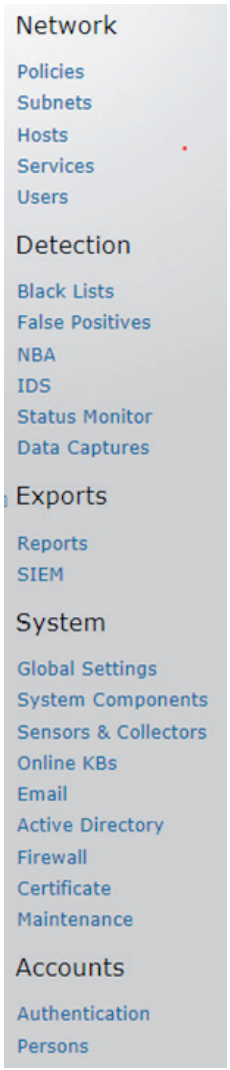
Aplikace je dodávána jako hardwarová „appliance“ nebo instalační ISO soubor do virtuálního hypervizoru. Podle způsobu nasazení je appliance dodávána se 2, 4 nebo 8 síťovými rozhraními umožňujícími monitorovat požadovaný počet zdrojových linek. Řešení může být nainstalováno v konfiguraci sonda – kolektor, která umožňuje monitorovat geograficky odlehlé sítě nebo jako cloud.

Produkt ve verzi 2.2.0 jsme testovali na Vysoké škole Karla Engliše (VŠKE), pro testování jsme si zvolili virtuální nasazení na bázi plně funkčního 30denního dema (uživatelskou příručku jsme měli pro verzi 3.0 [2], ale nějaké významné odlišnosti z hlediska ovládání jsme nenašli). Pro správný běh aplikace je třeba, aby server obsahoval procesor s nejméně 8 virtuálními jádry, 32 GB RAM, diskovou kapacitu o velikosti 500 GB a dvě síťová rozhraní; virtualizační systém byl VMware ESXi. Instalace proběhla zcela bez závad.

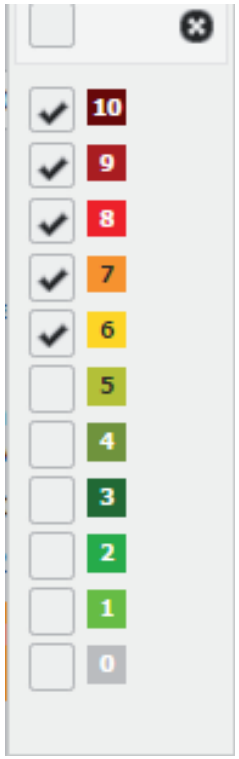
Záložky týkající se jednotlivých oblastí konfigurace jsou velmi přehledně umístěny, umožňují rychlý přechod na nastavení monitorovaných sítí a politik (záložka Policies), detekčních mechanismů (záložka Detection), hlášení a exportů (záložka Exports) a autentizačních mechanismů, uživatelů a jejich práv (záložka Users) – viz obr. 1. V záložce Network je praktické vhodné nastavení priorit – viz obr. 2.

Použití nástroje

Práce s aplikací GreyCortex je na první pohled velmi příjemná, především díky propracovaným možnostem filtrování a uživatelem libovolně konfigurovatelných přehledových dashboardů. Zaujala mne možnost rychlého zobrazení průběhu komunikace každého zařízení a všech jeho služeb.

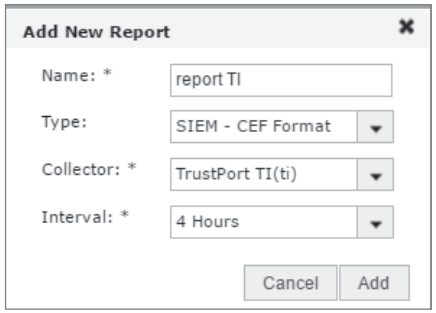


Obr. 1: Záložky týkající se jednotlivých oblastí konfigurace produktu GreyCortex

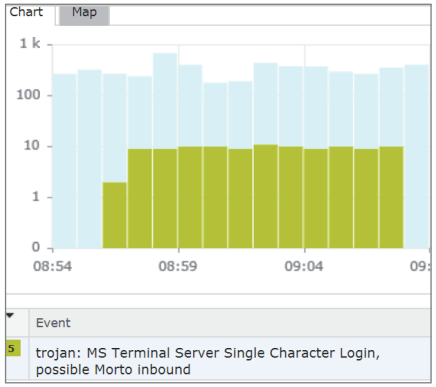


Obr. 2: Možná volba nastavení filtru priori

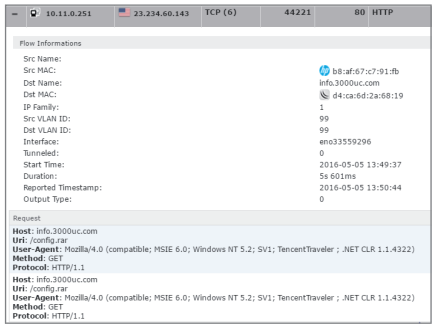
Samostatnou kapitolou je bezpečnostní viditelnost a přehlednost sítě, které aplikace přináší. Zobrazení incidentů detekovaných na úrovni detekčních vzorů je ideálně doplněna incidenty identifikovanými metodami NBA.



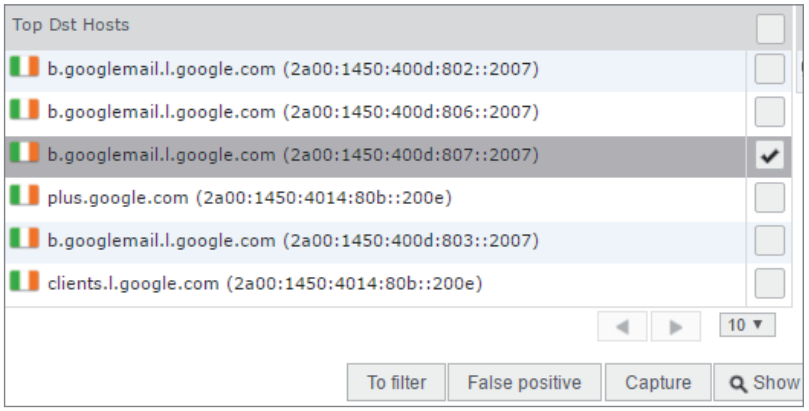
Obr. 3: Nastavení exportu do systému SIEM ve formátu CEF



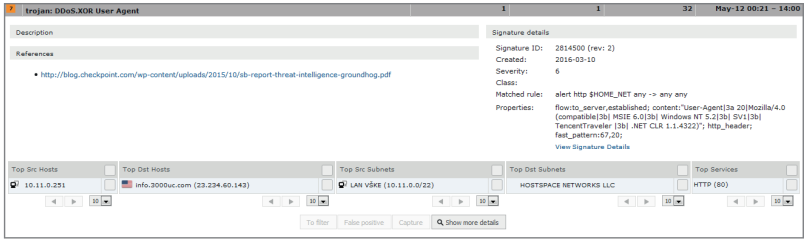
Obr. 4: Lze si zobrazit časový průběh útoku



Obr. 5: Lze provést detailní analýzu odchyceného malwaru – v tomto případě trojského koně



Obr. 6: Filtr na falešné poplachy pracoval naprosto spolehlivě



Obr. 7: Detekce DDoS trojského koně na Linuxovém serveru

Zařízení GreyCortex Mendel se prodává v cenách od 159 000 Kč za řešení bez bezpečnostních funkcí pro linky o kapacitě do 500 Mb/s, až po plnohodnotné řešení pro zpracování 10 Gb/s s uložištěm historie dat na 3 měsíce za více než 2 000 000 Kč.

V rámci záložky Detection si je možné zobrazit nastavené blacklisty a falešné poplachy, nastavit NBA detekční mechanismy a politiky u IDS pravidel, vytvořit potřebná korelační pravidla, zachytávat a ukládat síťový provoz na základě definovaného filtru do souborů formátu PCAP.

Záložka Export umožňuje definovat exporty – viz obr. 3, my na VŠKE provozujeme SIEM, proto pro nás byla zajímavá možnost exportu dat do tohoto systému. Zde jsme narazili na jednu potíž nepříjemnou zvláště pro školy – místo jedné aplikace nyní potřebujeme aplikace dvě – SIEM a GreyCortex.

Závěrečné poznámky

Co mě na tomto produktu zvláště těší, je možnost analyzovat dané incidenty (a že jich na škole ve studentské podsíti je) jak z hlediska jejich časového průběhu (obr. 4), tak do nejmenšího detailu (obr. 5). Dále musím ocenit kvalitní eliminaci falešných poplachů – viz obr. 6. Dokumentace splňuje základní požadavky, bylo by ji ale podle mne vhodné rozšířit o příklady typových nastavení. Produkt je stále rozvíjen, sám jsem zvědav, s čím novým ještě výrobci přijdou.

Jaroslav Dočkal
jaroslav.dockal@vske.cz

Doc. Ing. Jaroslav Dočkal, CSc.

Absolvent VDU Martin a VAAZ, v současnosti prorektor pro vědu a tvůrčí rozvoj a ředitel Ústavu informatiky na Vysoké škole Karla Engliše. Přednáší rovněž na Masarykově univerzitě a Univerzitě obrany, je lektorem Cisco akademie, školitelem HP a členem redakční rady DSM.

POUŽITÉ ZDROJE

[1] Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. National Institute of Standards and Technology February 12, 2014. Dostupné z: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf
[2] TrustPort: Threat Intelligence. User Guide v3.0. TrustPort 12/2015