GREYCORTEX

Zákon o kybernetické bezpečnosti

Jak pomáhá GREYCORTEX Mendel s naplněním opatření

Řízení aktiv

Identifikace technických aktiv a jejich vzájemných vazeb

Organizace musí mít přehled o všech zařízeních a systémech ve své infrastruktuře a o jejich vzájemné komunikaci. Stejně tak musí vědět o jakémkoliv jejich výpadku.

GREYCORTEX Mendel

- Provede snadno a rychle **audit všech technických aktiv.** Zjištěný stav porovnáte s inventárními záznamy organizace.
- **Detekuje a ukládá informace o každém zařízení** komunikujícím v síti.
- Zobrazí **seznam sítí a podsítí**, podrobně se podíváte, **která za**řízení do nich patří.
- Poskytne **podrobné informace o každém zařízení** jako hostname, funkce v síti, operační systém a další parametry.
- **Vizualizuje komunikační vazby** mezi jednotlivými hosty i do jakých segmentů jednotlivá zařízení komunikují.

Řízení rizik

Analýza rizik a identifikace kritických aktiv a služeb, jejichž výpadek může ohrozit provoz společnosti

GREYCORTEX Mendel

- Přiřadí každému zařízení **úroveň rizika** na základě automatické detekce, můžete ji přiřadit i manuálně dle vlastního vyhodnocení.
- **Vyfiltruje komunikační klienty**, které přistupují k určité službě nebo aplikaci jako podklad pro stanovení kritičnosti těchto služeb a aplikací.
- **Vizualizuje následky výpadku** konkrétního zařízení – jednoduše zjistíte, kolik zařízení nebude obslouženo v případě výpadku.

Bezpečnost lidských zdrojů a řízení přístupu

Kontrola dodržování bezpečnostních politik v souvislosti s životním cyklem zaměstnance

GREYCORTEX Mendel

- Je základem pro audit **chování uživatelů v síti**.
- Díky **integraci s nástroji pro správu aktiv nebo zdroji identit** vyvoříte seznam uživatelů a prozkoumáte jejich komunikaci s ostatními uživateli a službami.
- **Odhalí nepovolené přístupy:** Identifikuje komunikaci uživatele se systémem, ke kterému nemá mít oprávnění, přístupy přes VPN, přestože by jeho účet či vzdálený přístup měl být zablokován, přístup externího dodavatele do vnitřní sítě podniku, ke kterému dochází i po ukončení smlouvy, a další.

Provádění auditu kybernetické bezpečnosti

Pravidelná kontrola dodržování bezpečnostních politik a opatření

GREYCORTEX Mendel

- **Kontroluje dodržování** bezpečnostních politik a opatření **na denní bázi**.

Bezpečnost komunikačních sítí

Zajištění segmentace a integrity komunikační sítě, řízení komunikace v rámci interní sítě, vzdáleného přístupu a vzdálené správy

GREYCORTEX Mendel

- **Vizualizuje komunikaci zařízení**, snadno ověříte, zda zařízení z jedné podsítě nekomunikují neoprávněně se zařízeními z jiné podsítě nebo zda jsou přístupná z internetu, i když by neměla být.
- **Vyfiltruje komunikaci přes službu RDP**, která může být na firemní úrovni zakázána, i další služby.
- **Odhalí nelegitimní připojení**.
- Umožňuje **vynucování akčních kroků pomocí firewallu nebo NAC**, jako je například blokování komunikace, případě izolace zařízení.

Detekce kybernetických bezpečnostních událostí

Použití nástroje, který ověřuje a kontroluje přenášená data, řídí a sleduje komunikaci aplikací a služeb a detekuje kybernetické bezpečnostní události nad technickými aktivy

Jednou z hlavních schopností nástroje GREYCORTEX Mendel je detekce kybernetických bezpečnostních událostí, jejich zaznamenávání i vyhodnocování a zároveň účinná prevence incidentů. Mendel využívá pro detekci analýzu síťového provozu.

GREYCORTEX Mendel

- **Detekuje známé hrozby** na základě signatur.
- **Rozlišuje různé fáze jednotlivých kybernetických útoků** díky širokému rozsahu signatur a behaviorální analýzy.
- **Detekuje projevy nebezpečného chování** jako C&C odchozí komunikace, útoky hrubou silou, skeny, tunely a další.

Zaznamenávání událostí

Povinnost uchovávat záznamy událostí nejméně po dobu 18 měsíců

GREYCORTEX Mendel

- Zaznamenává všechny povinné údaje a umožňuje jejich dohledání **měsíce až roky do minulosti**. Omezeni jste jen velikostí vlastního úložiště.
- Umožňuje **nahrávání a export PCAP** pro využití záznamů v dalších nástrojích.

Vyhodnocování kybernetických bezpečnostních událostí

Využívání nástroje pro nepřetržité vyhodnocování kybernetických bezpečnostních událostí

Dle vyhlášky je nutné nepřetržitě vyhodnocovat kybernetické bezpečnostní události, což zahrnuje sběr záznamů, nepřetržité poskytování informací o událostech i jejich vyhodnocování s cílem identifikace kybernetických bezpečnostních incidentů.

GREYCORTEX Mendel

- **Umožňuje podrobnou analýzu** všech detekovaných událostí díky zobrazení mnoha detailů o událostech.
- **Kategorizuje všechny detekované události** podle MITRE ATT&CK Framework i řady dalších vizuálně srozumitelných pohledů a filtrů na vaše data.

Kryptografické algoritmy

Zajištění ochrany technických aktiv a jejich komunikace prostřednictvím nástrojů a mechanismů, které využívají kryptografii

GREYCORTEX Mendel

- Detekuje využívání neaktuálních a slabých kryptografických algoritmů
- Detekuje **nešifrovanou komunikaci** a **přenos hesel v plain-text formě**.
- Kontroluje **platnost komunikačních certifikátů**.

Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv

Paragraf shrnuje a zdůrazňuje nutnost zavedení veškerých bezpečnostních opatření také v průmyslových prostředích.

GREYCORTEX Mendel

- Poskytuje bezpečnostní **viditelnost do provozu průmyslových sítí** a kritické informace pro provoz výrobní infrastruktury, jako CVE, nežádoucí konfigurační nastavení zařízení nebo informace o změnách firmwaru.
- Zpracovává **OT protokoly** jako MODBUS, OMRON, BACnet a další.
- Vizualizuje **komunikaci zařízení až do úrovně 2 dle Purdue modelu** (senzory, čidla, motory a další)
- Poskytuje **informace o OT zařízeních** jako teplota pece, otáčky centrifugy, tlaky v potrubí, výška hladiny vody v nádobě a další.

Vyzkoušejte GREYCORTEX Mendel

Proof of Concept (PoC)

Ověřte si požadované funkčnosti Mendel na vlastní síti nebo její části. Lze rozšířit do úrovně bezpečnostního auditu sítě.

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

www.greycortex.com