COMGUARD
cyber security masters

CYREBRO

CYREBRO je průkopníkem prvního online, spravovaného Security Operations Center (SOC) a přináší kybernetickou bezpečnost enterprise úrovně pro společnosti všech velikostí, tato úroveň zajistí rychlé a efektivní reakce na kybernetické hrozby a jejich zmírnění.

CYREBRO SOC PLATFORM

Interaktivní platforma SOC společnosti CYREBRO integruje všechny protokoly z infrastruktury, sítě a cloudu do jedné centrální platformy, která poskytuje přehled o aktuálním dění a umožňuje podniknout kroky v reálném čase, aby mohlo dojít k nápravě či zmírnění detekovaných incidentů.

Unikátní vlastnosti:

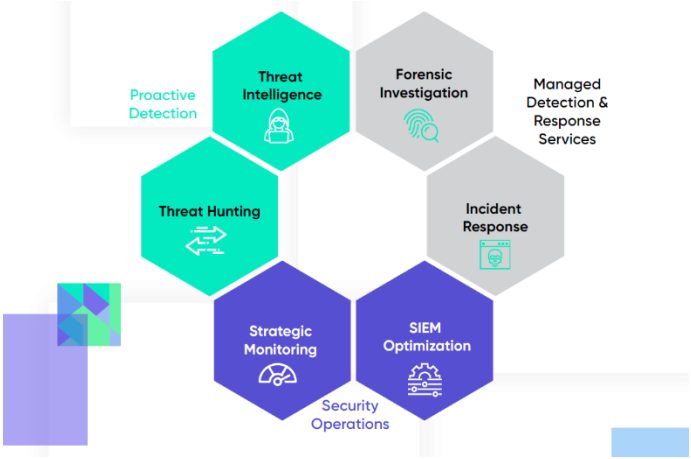
- Využití Data Lake
- Více než 1 500 jedinečných a proprietárních detekčních algoritmů, napsaných, testovaných a nasazených k detekci hrozeb v rámci kybernetických operací
- SIEM nové generace
- Interní automatizace a orchestrace
- Interní výzkum kybernetických hrozeb
- Interní zpravodajství o kybernetických hrozbách
- Sběr protokolu
- Podpora shromažďování protokolů napříč různými platformami a prost pokrývající stovky předních typů protokolů a systémů
- Proaktivní threat hunting
- CYREBRO navíc posiluje bezpečnostní týmy klienta tím, že poskytuje ochranu 24/7/365
- Pokročilé možnosti monitorování a vyšetřování incidentů
- Digitální analýza a reakce na kybernetické hrozby které jsou detekovány

Funkce SOC operací a vyšetřování

BEZPEČNOSTNÍ OPERACE

STRATEGICKÉ MONITOROVÁNÍ A DETEKCE

Přístup společnosti CYREBRO k monitorování, detekci a reakci je založen na kontinuálním učení, zlepšování a vyvíjení unikátních detekčních algoritmů. Zahrnuje kontinuální 24/7 monitorování organizačních aktiv, sítí a systémů. Přitom dochází k neustálému se z hrozeb a jejich případů použití po celém světě téměř reálném čase. CYREBRO je speciálně pro využití (Machine Learning), aby pomohl klientům zmírnit bezpečnostní rizika a efektivně provozovat svou infrastrukturu.



OPTIMALIZACE

Jedná se o proces neustálého zlepšování **CYREBRO SOC platformy**. Zahrnuje ladění komplexnosti systému, aby bylo zajištěno, že shromažďuje správná data, efektivně je analyzuje a poskytuje užitečné informace.

Cílem optimalizace je zlepšit přesnost a rychlost detekce hrozeb, snížit false positives a umožnit rychlejší odezvu na incidenty. Optimalizace je živý, probíhající proces v rámci „*CYREBRO Brain*", založený na kombinaci ML schopnosti, statistik a trendů s vysoce kvalifikovaným a zkušeným kybernetickým týmem v pozadí CYREBRO.

Optimalizace zahrnuje:

Zpřesnění upozornění/pravidel: Doladěním upozornění mohou organizace snížit počet „false positive" generovaných při identifikaci důležitých bezpečnostních událostí.

- Snížení chaosu: Odfiltrováním nepotřebných dat, jako je známý neškodný provoz popř. redundantní záznamy protokolu, CYREBRO se může zaměřit na události, které jsou nejvíce relevantní z ohledu bezpečnostni.
- Zvýšení viditelnosti dat: Shromažďováním a analýzou širšího spektra relevantních data událostí, včetně dat z cloudových prostředí a koncových bodů.
- Automatizace odezvy: Automatizací pracovních postupů reakce na incidenty, CYREBRO zkracuje dobu odezvy.

PROAKTIVNÍ DETEKCE

THREAT INTELLIGENCE

Poskytuje informace o hrozbách v rámci CYREBRO a je hlavním zdrojem relevantních a použitelných informací týkajících se potenciálních bezpečnostních hrozeb. Neustále vyhodnocuje relevantní ukazatele a potenciální hrozby v rámci každé jednotlivé technologie připojené k CYREBRO SOC platformě.

Mezi hlavní vlastnosti patří:

- Sběr dat o hrozbách: Shromažďování informací z různých zdrojů, např. interní bezpečnostní protokoly, externí informační kanály o hrozbách a open-source zdroje.
- Analýza hrozeb: Analýza shromážděných dat k identifikaci potenciálních hrozeb, za účelem odhalení vzorů útoků a indikátorů kompromitace (IOC).
- Sdílení informací o hrozbách: CYREBRO informuje o hrozbách formou zprávy, výstrahy a rady příslušným zainteresovaným stranám v rámci CYREBRO, včetně týmu pro reakci na incidenty a bezpečnostních analytiků.

THREAT HUNTING

Proces vyhledávání hrozeb společnosti CYREBRO je založen na proaktivním přístupu k identifikaci potenciálu kybernetické hrozby. Zahrnuje hledání indikátorů kompromitace (IOC) a další anomální aktivity, které by jinak mohly zůstat bez povšimnutí za použití tradičních bezpečnostních opatření.

Zahrnuje tzv. *„wisdom of the crowd*", využití zkušeností v minulosti řešených kybernetických hrozeb a nyní probíhající případy spolu s rozsáhlými zkušenostmi.

Proces vyhledávání hrozeb zahrnuje zpracování obrovského množství dat z různých zdrojů. Data jsou poté analyzována, aby se identifikovaly vzorce, anomálie a potenciál MOV, které mohou naznačovat přítomnost bezpečnostní hrozby.

MANAGED DETECTION AND RESPONSE SERVICES

INCIDENT RESPONSE

Reakce CYREBRO na incidenty poskytuje organizacím efektivní přístup k řízení bezpečnostních incidentů. CYREBRO tým anaytiků se zkušenostmi ze státní i soukromé sféry provádí stovky IR operací po celém světě, nehledě na velikost či úroveň složitosti. CYREBRO se řídí dobře definovaným procesem, který zahrnuje přípravu, identifikaci, omezení, analýzu a obnovu za účelem dosažení optimálních výsledků včasným a spolehlivým způsobem.

CYREBRO po konzultaci se zákazníkem klasifikuje úroveň závažnosti incidentu. Pokud je to vhodné, tým IR sestaví a poskytne klientovi komunikační protokol, který umožní komunikaci související s incidentem pro příslušné skupiny. Označení incidentů a jejich zařazení:

- Určení a nasazení vhodné strategie jak reagovat na daný incident
- Společnost CYREBRO incident vyšetří, zamezí dalšímu působení a vyřeší daný incident
- Spolupráce na kontrole a uzavření incidentu
- Kontrola a aktualizace IRP zákazníka dle jeho potřeby

V případě bezprostřední hrozby, jako je například probíhající živý kybernetický útok na organizace, je tým k dispozici 24 hodin denně, 7 dní v týdnu, aby mohl ihned reagovat na bezpečnostní incident a následně po jeho identifikaci incident vyřešil.

Každá vyhodnocená IR bude obsahovat úplnou „postmortem" podrobnou zprávu o událostech incidentu

DIGITAL FORENSICS

Digitální forenzní analýza společnosti CYREBRO poskytuje organizacím důkladný a efektivní přístup k vyšetřování a analýze digitálních stop a důkazů souvisejících s bezpečnostími incidenty. V našem procesu dodržují digitální forenzní analytici přísný postup který zahrnuje získávání, uchovávávání, analýzu a reporting.

CYREBRO připraví podrobnou zprávu, která nastiňuje výsledky vyšetřování, včetně popisu incidentu a metod použitých k získání a analýze důkazů. Vyhodnotí potenciální právní nebo regulační důsledky které incident mohl způsobit. Také poskytuje doporučení pro zlepšení bezpečnostní pozice organizace a prevence k podobným incidentům v budoucnu.