COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

LABYRINTH

Nechť jsou klam a faleš vaší účinnou zbraní proti bezpečnostním hrozbám. Deceptivní technologie firmy Labyrinth vám poskytne velkou výhodu proti kybernetickým útokům. Budete zdržovat útočníka návnadou v podobě zajímavých, ale falešných dat a útočník na sebe při práci s těmito daty okamžitě upozorní. Tato technologie je jako minové pole. Jakmile do něj útočník vstoupí je v pasti i když o tom ještě neví. Systém ho bude na každém kroku blokovat a mapovat jeho činnost. A to vše v kompaktní, přehledné a jednoduché platformě, která nepracuje s daty a nebude tak vyžadovat žádnou zvláštní péči i když bude trvale ochraňovat vaši infrastrukturu.

Labyrinth to je tým inženýrů zaměřených na kybernetickou bezpečnost a penetrační testování, kteří se zaměřují na rychlou detekci hrozby a prevenci před ní. Jejich cílem je poskytnout organizacím jednoduchý a efektivní nástroj pro brzkou identifikaci hrozby.

Labyrinth se zabývá problematikou kybernetické bezpečnosti za použití technologie deception, která provádí detekci a blokaci útoků, a to bez falešné pozitivity. Tuto problematiku řeší díky své platformě na klam a iluze. Tato bezpečnostní platforma slouží k odhalování propracovaných útoků používáním návnady (falešná endpoint zařízení, data, linky, ssh klíče, disky, ...) a to tak abychom navýšili pravděpodobnost toho, že se útočník chytí do pasti a půjde po těchto zajímavějších datech, které slouží také k odhalení jeho nekalé činnosti. Umyslně krmíme útočníka daty abychom ho nalákaly do pasti.

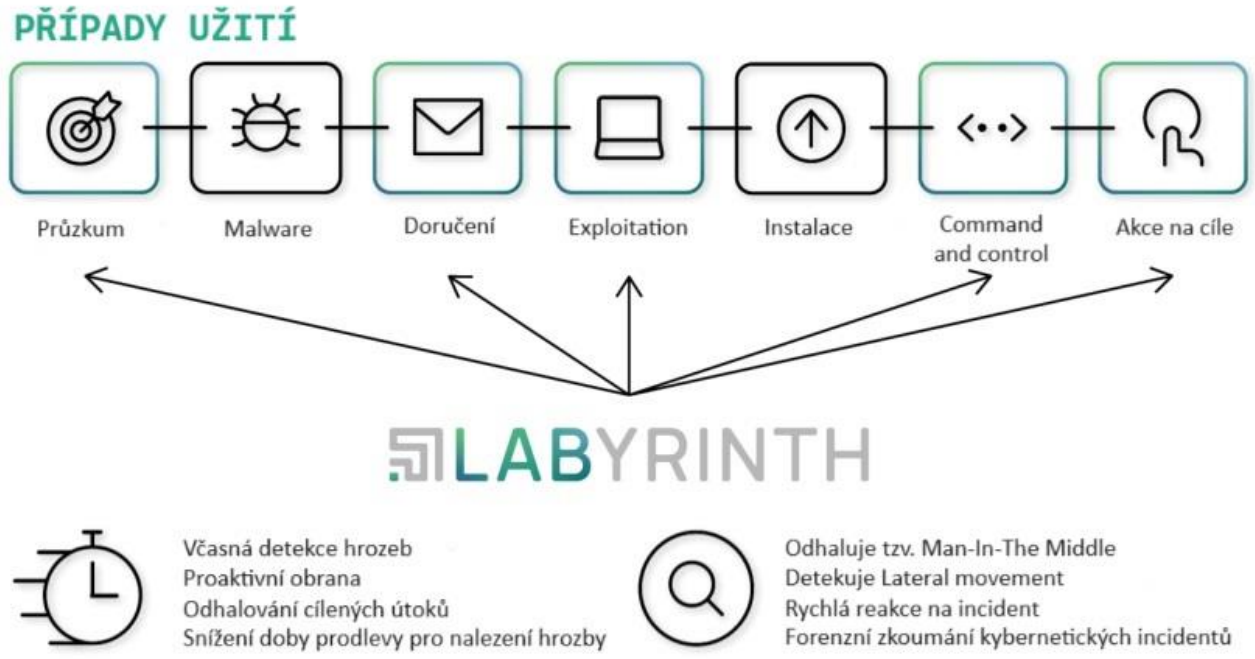
Útočníkovy budou připadat falešná data a další prvky zajímavější a dostupnější díky tomu, jak reálně budou vypadat a chovat se jako skutečná. V této umělé konstrukci dochází i k napodobení celé sítě. Řešení od Labyrinthu vytvoří oslabené vstupy, které útočníka vedou k zajímavějším údajům, které budou pro něj snadné cíle. Každá tato návnada je jedinečná a vysoce interaktivní po textové a grafické stránce. Jakmile ale některou z nich útočník použije vyvolá se hlášení o narušení bezpečnosti na což může následně technický tým rychle reagovat. Dále také zastaví útočníkův postup díky propojení s produkty třetích stran (např. Windows nebo Trellix).

Systémové požadavky: VMware vSphere 6.0/6.5/7.0, Microsoft Hyper-V 2008 R2 a vyšší, Microsoft Azure Cloud. Oficiální podpora AdminVM na KVM založených platformách (Proxmox, OpenStack, atd.).

Klíčové vlastnosti řešení

- Detekuje, zastavuje cílené a pokročilé kybernetické útoky bez nutnosti předešlých znalostí formy, typu a chování této hrozby – zero day attack
- Viditelnost útoku v reálném čase a v přehledné podobě
- Automatická detekce a odpověď na hrozbu, pokud je tato platforma integrována s nástroji třetí strany
- Nesbírá tuny dat, používá pouze data o incidentech
- Negeneruje falešně pozitivní hlášení
- Pro užívání nejsou nutné speciální schopnosti a ani vysoká odbornost
- Zkracuje reakční rychlost na incidenty jak pro objevení hrozby, tak i na odpověď na ni (MTTD, MTTR) a to 12x oproti běžným metodám detekce.
- Každá klamná iluze je jedinečná a působí realisticky díky fiktivní činnosti zařízení
- Žádný negativní dopad na funkčnost a chod síťových zařízení, hosts, serverů a aplikací
- Rychlé a snadné nasazení – žádný konflikt se systémem
- Není nutná údržba – žádné databáze, signatury ani pravidla pro neustálou konfiguraci a update.

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

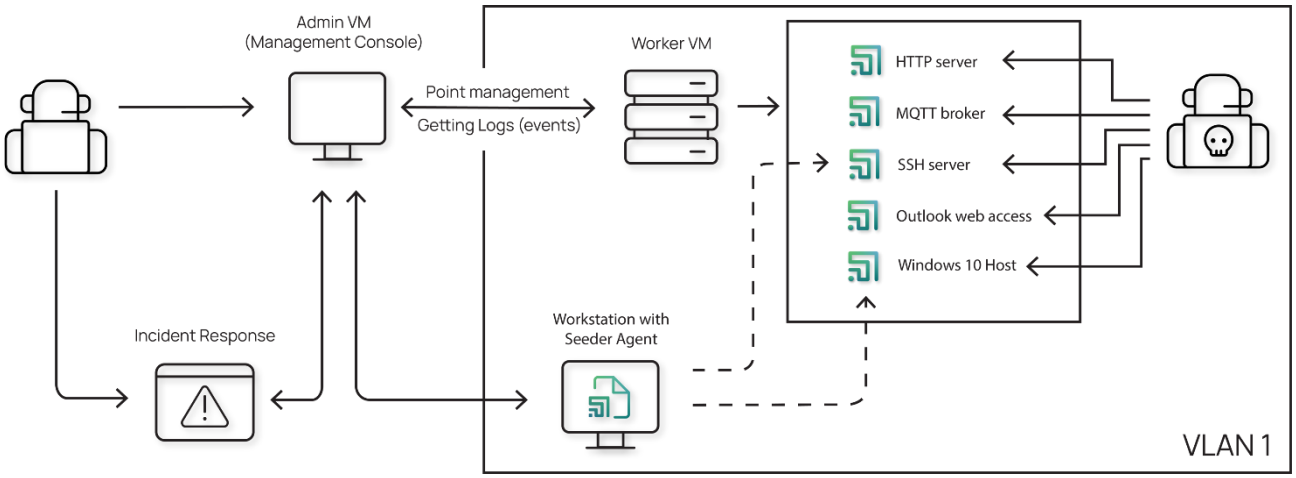


Stand-alone – může být použito jako samostatné řešení pro implementaci detekce. Propojení s produkty třetí strany NGFW a EDR, které napomohou akceleraci rekční doby na incident, forenzní šetření a možnost automatického odeslání nezbytných dat do IRMS.

SOC – sesbírá data o incidentech a pošle je do SIEM. Integrace se SIEM vytváří příležitost získat dodatečné informace o detekci podezřelé aktivity, čímž se zlepší viditelnost řetězce bezpečnostního incidentu.

MSSP – Labyrinth může pracovat jako klient, zatímco Admin Server, IRMS, SIEM – umožní MSSP poskytovat plnou konfiguraci a pozorování aktuální situace subsystémů. V případě integrace se systémy třetích stran (NGFW, EDR, WAF, atd.), která napomůže akceleraci a reakce na incident je tak možná okamžitě po jejich detekci bez nutnosti zapojení technika.

Architektura řešení systémem Labyrinth



IČ04305426, DIČ CZ04305426, OR KS v Brně značka B. 7361