Attivo NETWORKS®

ThreatDefend Detection & Response Platform

Kde je vůle, je i cesta. To bohužel platí i v kontextu cesty za hranice perimetrové obrany a na ně navazujících aktivit hackerů. Platforma ThreatDefend zajišťuje vhled do aktivit útočníků uvnitř hranic společnosti, kterou dále doplňuje o bezprecedentní obranu před odcizením identit, eskalací privilegií a provádění laterálních pohybů díky využití taktik útočníků samých. S ThreatDefend může být každý počítač ve Vaší síti efektivní pastí generující relevantní upozornění na aktivity útočníků, navíc zcela bez zbytečného šumu a false positives, čímž výrazně přispívá k úsporám personálních kapacit bezpečnostních teamů.

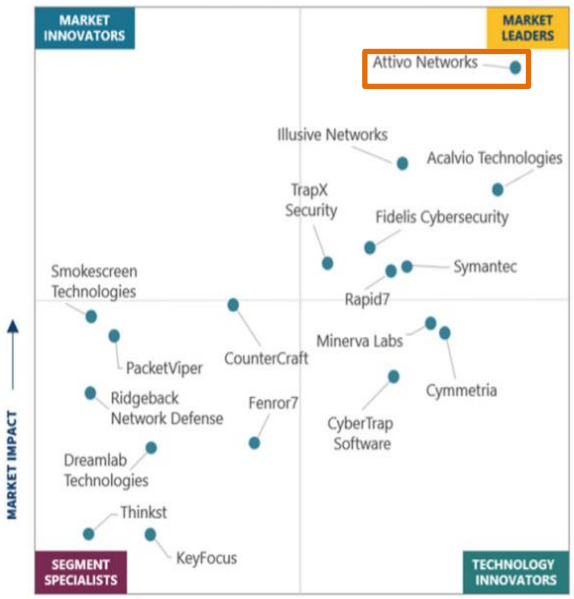
Technologie klamu jako aktivní prvek obrany

Nepřeberné množství úspěšných kybernetických útoků poukázalo na fakt, že bezpečnostní strategie spoléhající na běžné preventivní a detekční mechanismy nemusí být všespásná. Konvenční metodiky pro detekci hrozeb uvnitř podnikové sítě trpí vysokou komplexitou nebo nízkou mírou přesnosti, díky které generují alerty v kvantitě, která vede k jejich postupné ignoraci. Tím dopřávají aktérům útoků desítky, ne-li stovky dní prostoru mezi prvotním průnikem a vykonáním záměru. Tento čas je využit pro mapování prostředí, identifikaci kritických systémů a dohledání hodnotných dat.

Techniky klamu předpokládají, že je průnik nevyhnutelný a útočníkovi předkládají prvky, které vedou k neprodlené detekci, odklonění útoku do detonačního prostředí a odhalení taktik a procedur, které byly během útoku využity. Takováto míra opakovaného narušení útočné sekvence zcela mění ekonomickou výhodnost situace a útočníka úspěšně odrazuje od dalších aktivit.

Attivo ThreatDefend Platform

Pro efektivní působení klamných prvků je klíčové široké pokrytí a vysoká míra jejich autentičnosti, která zamezí jejich detekci a podpoří útočníka v další interakci. V obou těchto oblastech je Attivo Networks se svou platformou ThreatDefend dlouholetým leaderem a k nejobsáhlejšímu setu návnad s využitím reálných systémů, aplikací, účtů či adresářových služeb přidává pokročilé prvky pro obfuskaci reálného stavu a forenzní analýzu. Díky své koncepci a umístění mimo běžný pracovní prostor tak **ThreatDefend generuje alerty pouze v případě nežádoucí aktivity**. Pro urychlení a automatizaci reakcí a nápravných opatření pak přidává širokou paletu nativních integrací s bezpečnostními systémy třetích stran či mapování nálezů na matici MITRE ATT&CK frameworku. Modularita a skvělá škálovatelnost tohoto řešení pak v kombinaci s využitím strojového učení pro návrh architektury zajišťují snadné nasazení v organizaci libovolného rozsahu.



Endpoint Detection Net

Sada nástrojů EDN byla vyvinuta s cílem aktivně předvídat kroky útočníka na úrovni prvního nakaženého stroje a zamezit provádění průzkumu a laterálních pohybů. Využívané metodiky nijak nespoléhají na signatury a IOC- místo toho z každého koncového bodu udělají návnadu pomocí pokrytí vektorů šíření. Tento přístup je mimořádně efektivní jako doplněk stávající kaskády EPP / EDR.

ThreatStrike je komponenta pro zanechání návnad na úrovni koncových bodů. Tyto vysoce přizpůsobitelné návnady mohou zahrnovat cachovaná hesla, hashe či síťové disky pro detekci a „zaneprázdnění" ransomware, které vede k ochromení útočné kapacity. Interakce s návnadami neprodleně vyvolává alert v EDN Manageru.

ADSecure zamezí nežádoucímu vyčítání dat z Active Directory díky mechanismu zachycujícímu AD queries. ADSecure skryje zachytí odpověď produkčního AD a nahradí jí klamavými informacemi, čímž útočníka odkloní od produkčního prostředí k Engagement Serverům a následně vygenerují alert bezpečnostnímu teamu.

ThreatPath aktivně vyhledává prvky umožňující laterální pohyby a vizuálně mapuje dosah přihlašovacích údajů včetně orphaned credentials pro detekci a pochopení možných tras útočníků. Integrace s nástroji třetích stran následně umožní snadné zmenšení útočného povrchu.

Deflect upozorní na průzkumné fáze založené na scanování portů a detekci běžících služeb. Tento typ komunikace umožní oboustranně přesměrovat pro obfuskace prostředí a odklonění útočníka. Tento mechanismus izoluje útočníka díky omezení možnosti komunikovat pouze na interaktivní Engagement servery.

DataCloak aktivně chrání data prostřednictvím skrývání a odpírání přístupu k produkčním souborům, složkám, vyměnitelným médiím, síťovým diskům a cloudovým úložištím. DataCloak dále zabraňuje detekci lokálních administrátorských účtů pro zamezení eskalace privilegií.

COMGUARD security & networking

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

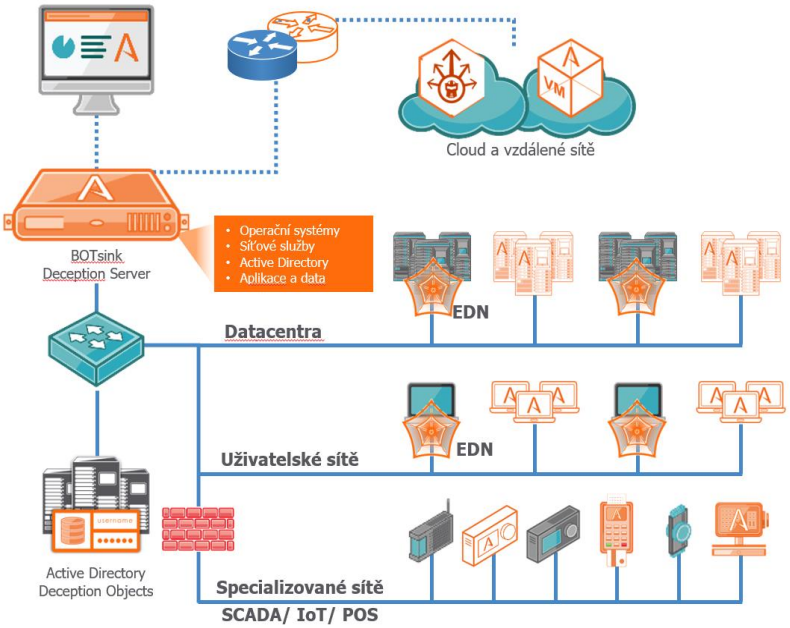
Attivo NETWORKS®

ThreatDefend Detection & Response Platform

BOTsink

Technologie BOTsink rozšiřuje EDN o vysoce přizpůsobitelnou síť návnad, na které jsou směřovány všechny modifikované útočné vektory. Jako návnady lze využít existující Gold Images, či předpřipravené systémy- Koncové body, servery, aplikace, databáze, Active Directory, IOT, ICS, POC či další specifické systémy. Nasazení je usnadněno pokročilým mechanismem pro analýzu reálného prostředí, který díky machine learningu navrhne podobu klamných prvků.

Tyto návnady následně vytváří sandboxové prostředí, které podpoří útočníka v interakcích pro následné poskytnutí dat, podkladů a informací o jejich technikách, taktikách a procedurách. Informace získané prostřednictvím BOTsink jsou mapovány na matici MITRE ATT&CK pro snazší analýzu a případné integrace s procesy SOC teamu. Široká škála předpřipravených integrací s bezpečnostními nástroji třetích stran dále zajišťuje pokročilé možnosti hloubkové analýzy, orchestrace reakcí, blokování či umísťování do karantény.



Hlavní výhody řešení

- Snadné nasazení a škálovatelnost
- Nízké provozní nároky
- Pouze relevantní alerty s potřebným kontextem
- Široký ekosystém partnerských integrací
- Rychlá detekce všech vektorů útoku
- Okamžitý náhled do zneužití a zcizení credentials
- Detailní forenzní analýza
- Komplexní pokrytí in-network aktivit dle MITRE ATT&CK

ThreatOps – Nativní partnerské integrace pro automatizaci reakcí na incidenty

Reakce: Síťové blokace

Check Point SOFTWARE TECHNOLOGIES LTD. · Cisco · Fortinet · Juniper Networks · paloalto networks. · Symantec BLUE COAT

Distribuce ThreatStrike

McAfee · Tanium

Endpoint management solutions such as SCCM, WMI, Casper, and others

Integrace s Attivo API

Digital Defense Incorporated

Investigace: Analýza & ThreatHunting

FireEye · Forescout · IBM Radar · LogRhythm · McAfee · Micro Focus · ReversingLabs · Splunk> · Tanium · ThreatConnect · VirusTotal · Webroot an opentext company

Orchestrace

Cortex XSOAR by Palo Alto Networks · Resilient an IBM Company · Splunk> phantom · Swimlane

Reakce: Endpoint Quarantine

McAfee · Cisco · CrowdStrike * · FireEye · Forescout · aruba a Hewlett Packard Enterprise company · GoSecure powered by Countertack · Tanium · vmware Carbon Black.

Cloud Monitoring

box · Google Drive · Office 365 · salesforce

Přesměrování

McAfee

Ticketing

servicenow

COMGUARD security & networking

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