Acalvio ShadowPlex

Hrací pole kybernetických hrozeb není férově postavené. Jako obránci musíme být ve 100 % případů neomylní, pokročilému útočníkovi mnohdy stačí naše jediné pochybení pro upevnění pozice uvnitř perimetru. Efektivním řešením této problematiky je aktivní obrana s využitím vysoce přesvědčivých klamných prvků, které útočník nedokáže rozeznat od zamýšlených cílů – Jakýkoliv kontakt s nimi následně vyvolá přesný alert – Bez šumu či false positives.

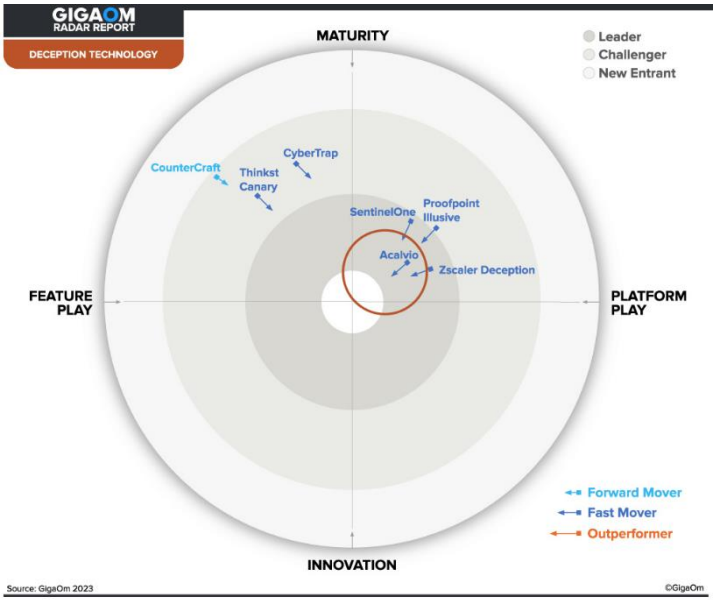
Techniky klamu jako prvek aktivní obrany

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.)

Acalvio ShadowPlex

Leader v oblasti Deception Technologies, společnost Acalvio, postavila svou platformu ShadowPlex na 25 patentovaných mechanismech, díky kterým umožní velmi snadno rozšířit cíl útoku, tedy produkční infrastrukturu o „zrcadlové bludiště" klamných prvků. Po prvotním automatizovaném scanu jednotlivých síťových segmentů vygeneruje ShadowPlex návrh skladby klamných prvků založený na reálném stavu. Do sítě s PC jsou přidána klamná PC, do serverových sítí klamné servery. Obdobný přístup dokáže aplikovat i u adresářových služeb, databází, síťových služeb, OT / IoT prvků, aplikací či v cloudových prostředích. Do tohoto detonačního prostředí útočníka směřují návnady rozmístěné na produkčních strojích, jejichž generování je taktéž plně automatizováno s možností manuálních úprav v případě potřeb.



Skladba klamných prvků na úrovni produkčních strojů zahrnuje artefakty, které útočník typicky vyhledává a využívá při dalších krocích – Uložená hesla, mapované disky, zápisy v registrech a desítky dalších. Díky umístění klamných prvků mimo standardní pracovní prostor lze každou interakci s nimi považovat za nežádoucí aktivitu, Acalvio proto prakticky negeneruje false positives.

V případě detekce hrozby poskytuje řešení graficky znázorněný přehled nálezů pro usnadnění orientace a rychlou reakci, která může být díky široké paletě integrací s nástroji jako EDR / XDR, SOAR, NAC či FW i částečně automatizovaná. Součástí informací o detekované hrozbě je i kompletní přehled prvků, které mohla daná kompromitace postihnout také – Díky propojení systémů či možnosti využití odcizených přihlašovacích údajů.

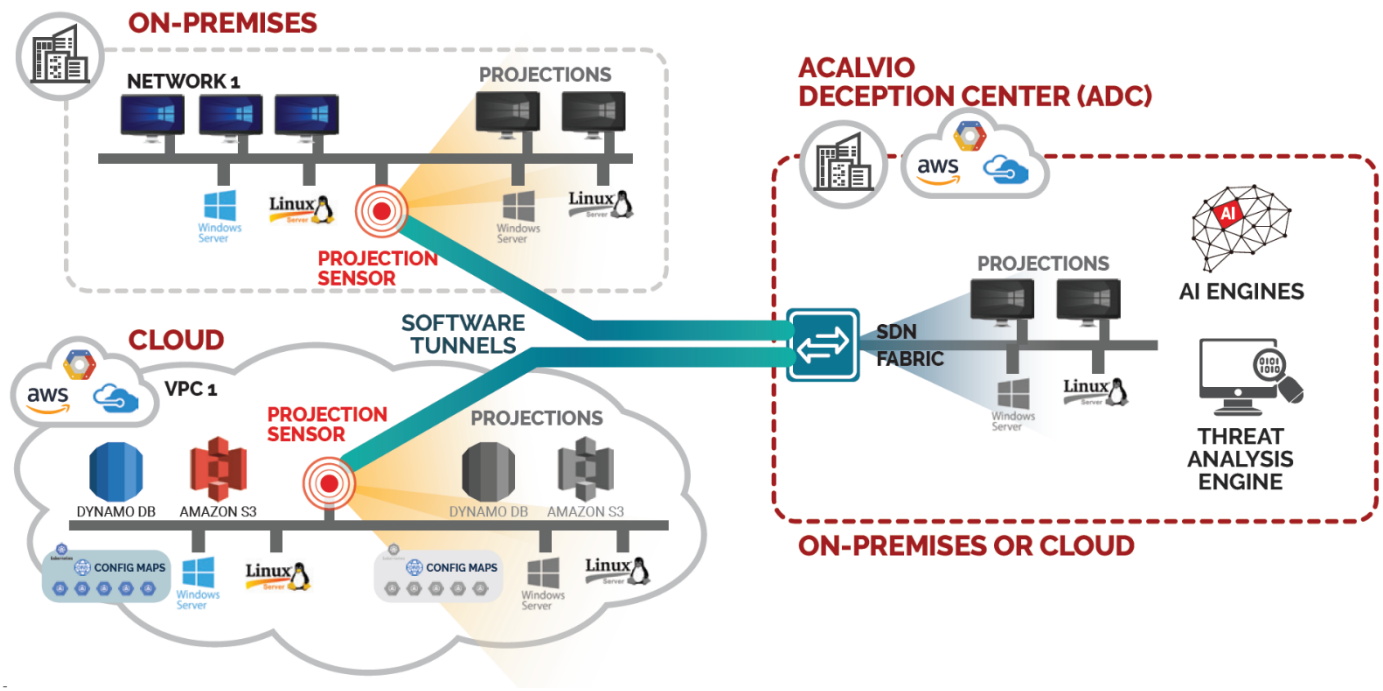
COMGUARD
communication security

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

COMGUARD

ACALVIO

Acalvio ShadowPlex



Architektura

Základní modul ADC (Acalvio Deception Center) je dostupný on-premise jako virtuální appliance či v cloudu (SaaS / vlastní cloud, možnost využití EU datacenter). Obsahuje management, prostředí pro analýzu hrozeb a Projections, tedy jednotlivé síťové návnady jako PC, servery, databáze, aplikace. Ty následně promítá na cílové adresy napříč relevantními segmenty sítě a v případě interakce útočníkem dále neumožňuje návrat do produkční infrastruktury.

Pro odklonění útočníka od reálných cílů a včasnou detekci jsou využity různé druhy klamných prvků – Projections věrohodně napodobují reálná zařízení a služby, jsou jim přiřazeny adresy, generují síťový provoz. **Breadcrumbs** jsou bezagentsky distribuovány na koncových bodech a útočníka vedou přímo k Projections. Na koncových bodech mohou být umístěny i **Baits**, které při interakci vyvolají alert. V neposlední řadě jsou využity **Lures**, které zajistí atraktivitu klamného prostředí a útočníka odkloní od reálných cílů.

PROJECTIONS
Servery
Pracovní stanice
Aplikace
Databáze
Vlastní images
Síťové služby

BREADCRUMBS
Zápisy v registrech
Složky a soubory
Credentials v paměti
Historie prohlížeče
Mapované disky
Úložiště hesel

BAITS
Beaconing dokumenty
Složky a soubory
DNS záznamy
Databázové záznamy
Monitorované procesy

LURES
Zranitelnosti
Chybné konfigurace
Defaultní či slabé credentials
Chybně nastavená oprávnění
Názvy prvků

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

COMGUARD
communication security

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