COMGUARD

cyber security masters

Acalvio ShadowPlex

Techniky klamu jako budoucí standard

Lukáš Babčický

18.09.2023

Dwell time

Časový úsek od momentu průniku do momentu detekce

	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
All	**416**	**243**	**229**	**205**	**146**	**99**	**101**	**78**	**56**	**24**	**21**	**16**
External	–	–	–	–	320	107	186	184	141	73	28	19
Internal	–	–	–	–	56	80	57.5	50.5	30	12	18	13

M-TRENDS 2023
MANDIANT SPECIAL REPORT

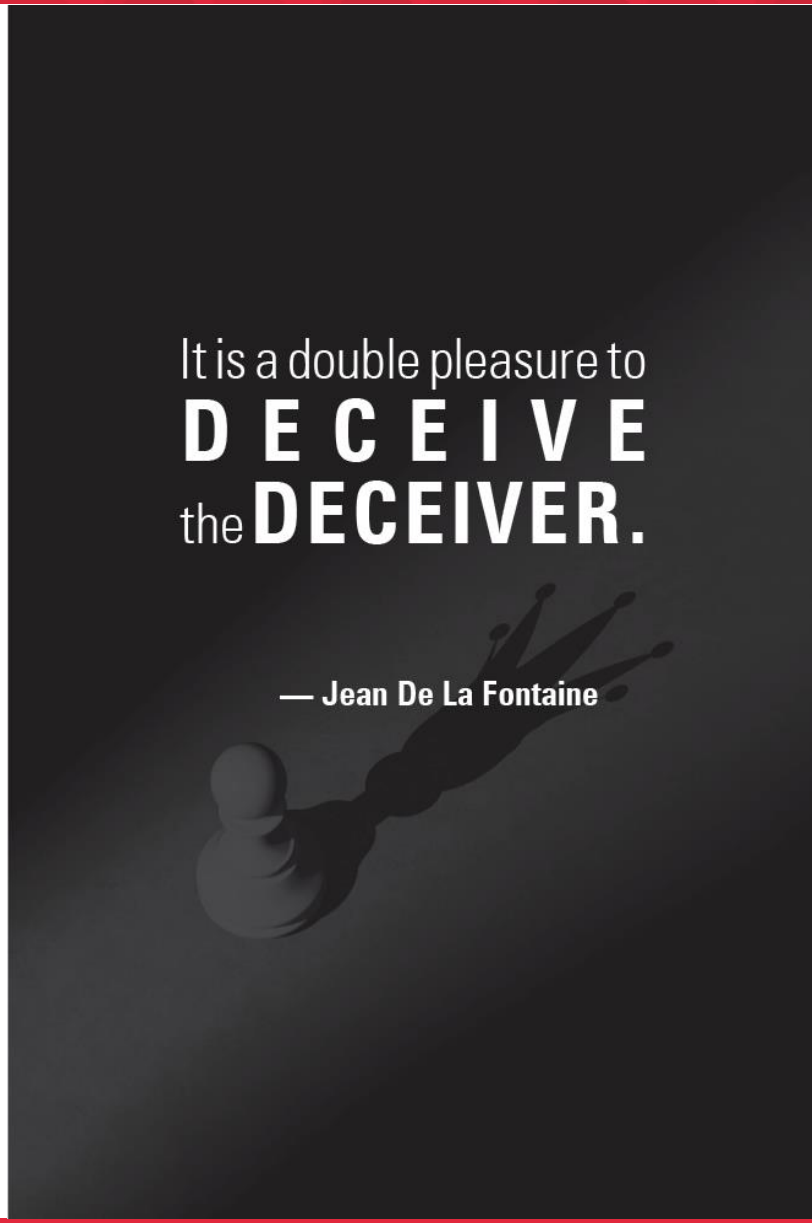
Zdroj: Mandiant M-Trends 2023

Dwell time

- Prostor pro průzkumnou aktivitu útočníka
- Discovery (průměrně 90 minut)
  - Sběr informací o systému, síti, adresářových službách
  - Hledání zneužitelných zranitelností
  - Kompromitace přihlašovacích údajů, boční pohyby, eskalace privilegií
  - Obtížně detekovatelné konvenčními nástroji
  - Z průniku na doménového administrátora během několika hodin?

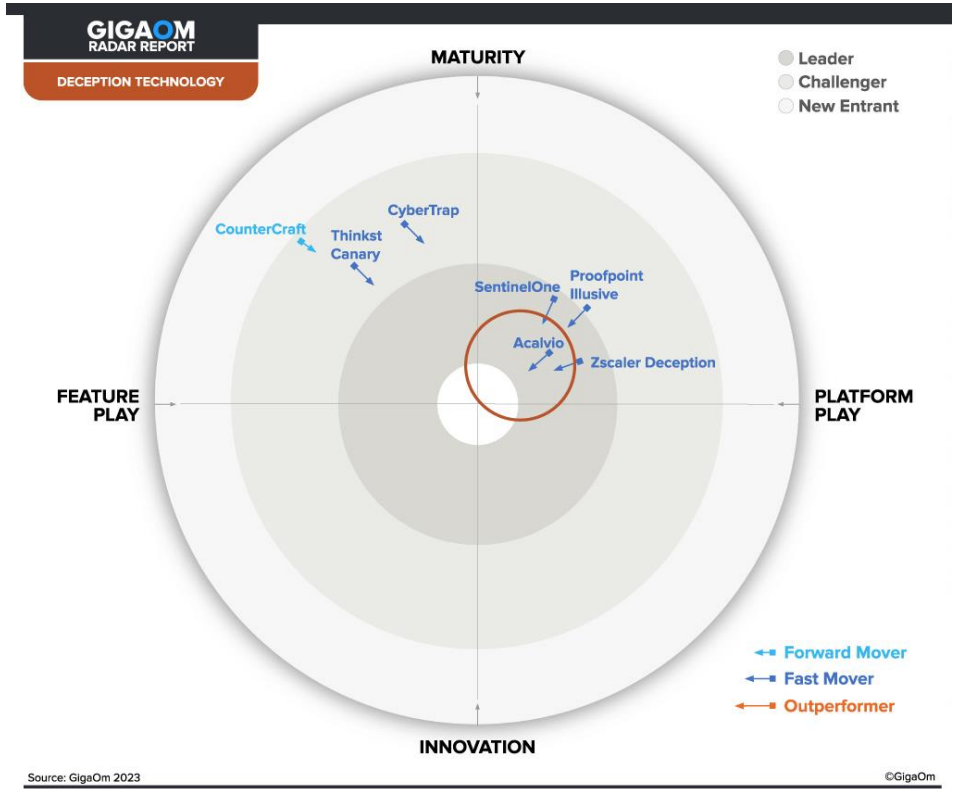
Techniky klamu

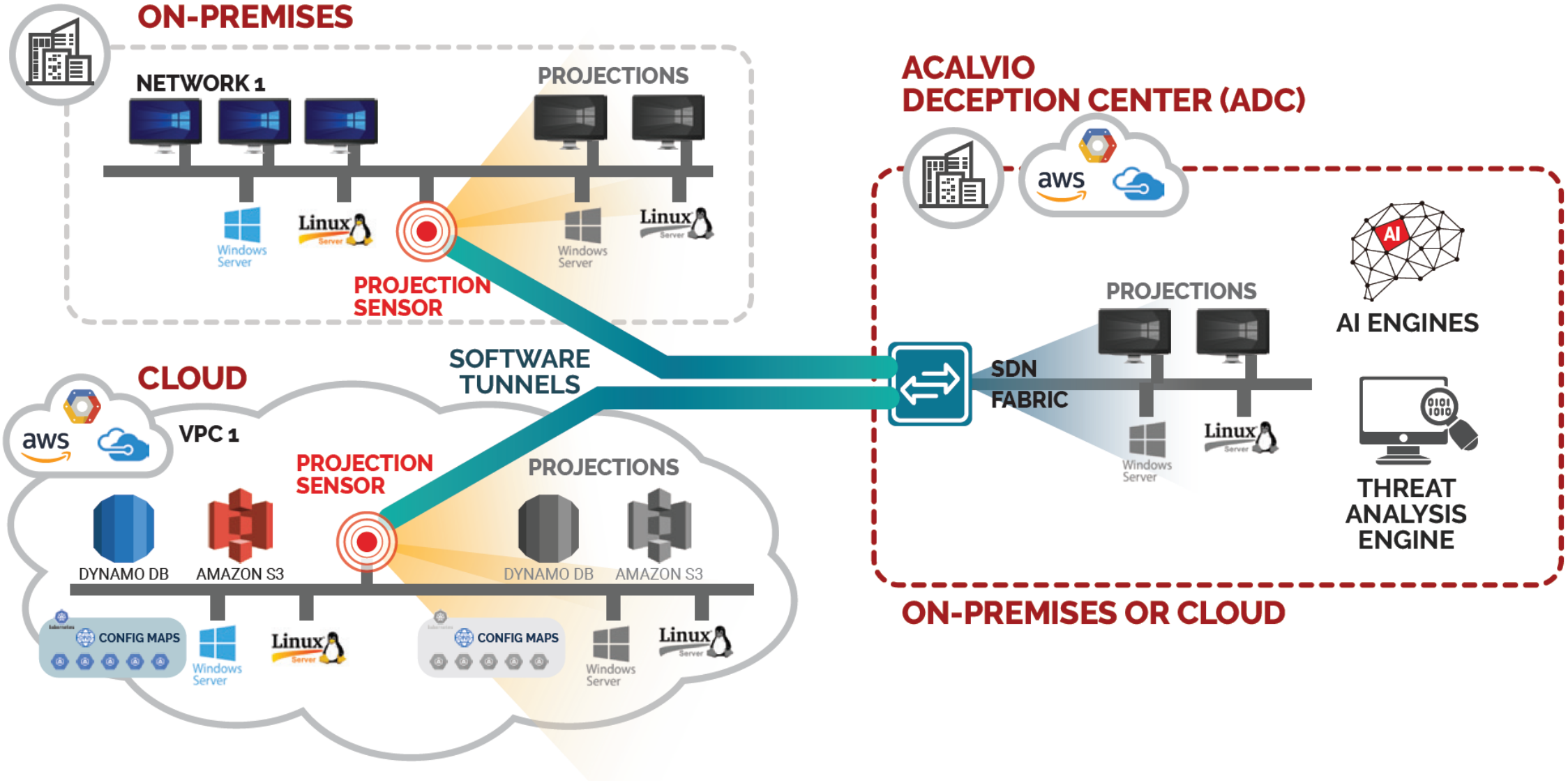
- Předpokládají nevyhnutelnost kompromitace
  - Předkládají útočníkovi povržené informace pro ovlivnění jeho dalších kroků
  - Odklonění útoku, zdržení a vyčerpání útočníka
  - Okamžitá detekce při interakci s návnadou



ShadowPlex – Deception platform / ITDR

- **Leader v oblasti Deception Technologies.** Autonomně navrhne, nasadí a spravuje „zrcadlové bludiště" klamných prvků s vysokou mírou interaktivity.
- **Flexibilita.** Ochrana on-premise i v cloudu, standardní i specializovaná zařízení, IT / OT, včetně doposud nechráněných prvků.
- **Urychlení reakcí a zkrácení dwell time**. Kompletní pokrytí matice MITRE ENGAGE, snadná integrace se zbytkem bezpečnostního ekosystému.




ON-PREMISES
NETWORK 1
PROJECTIONS
Windows Server
Linux Server
PROJECTION SENSOR
SOFTWARE TUNNELS
CLOUD
aws
VPC 1
PROJECTION SENSOR
PROJECTIONS
DYNAMO DB
AMAZON S3
CONFIG MAPS
ACALVIO DECEPTION CENTER (ADC)
SDN FABRIC
AI ENGINES
THREAT ANALYSIS ENGINE
ON-PREMISES OR CLOUD

Projections

- Servery
- Pracovní stanice
- Databáze
- Active Directory
- OT prvky
- Aplikace
- Tiskárny

- Interaktivní a dynamické prvky pro engagement, intel a vyčerpání

Breadcrumbs

- Historie prohlížečů
- Uložená hesla
- RDP profily
- Zápisy v registrech
- ARP cache

- Vodítka směrem k Projections

Baits

- Honey accounts
- Honey tokens
- Mapované disky
- Monitorované soubory
- Tainted tools

- Okamžitá detekce s první interakcí

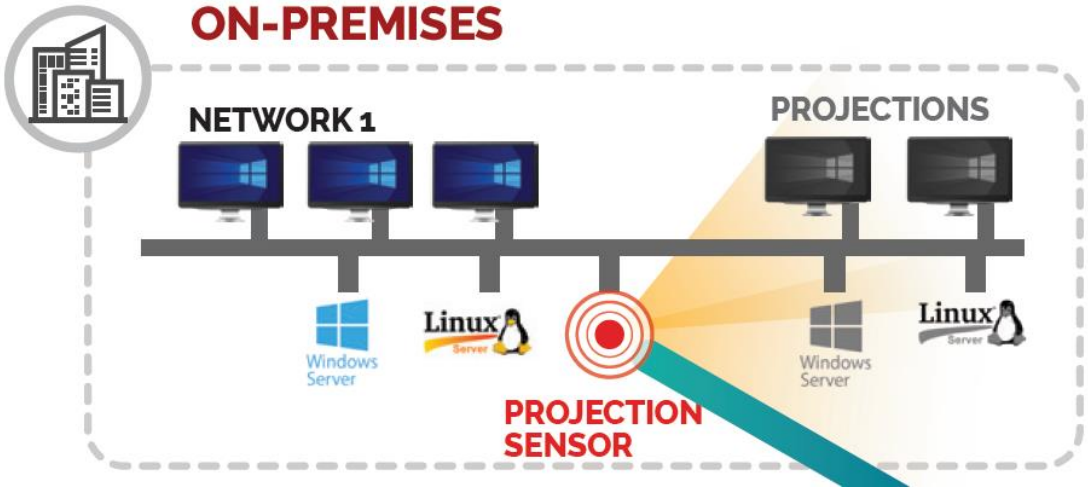
Doprovodné funkcionality

- Traffic mezi návnadami
- Bonjour
- LLMNR

- Mažou rozdíly mezi reálnou a klamnou částí

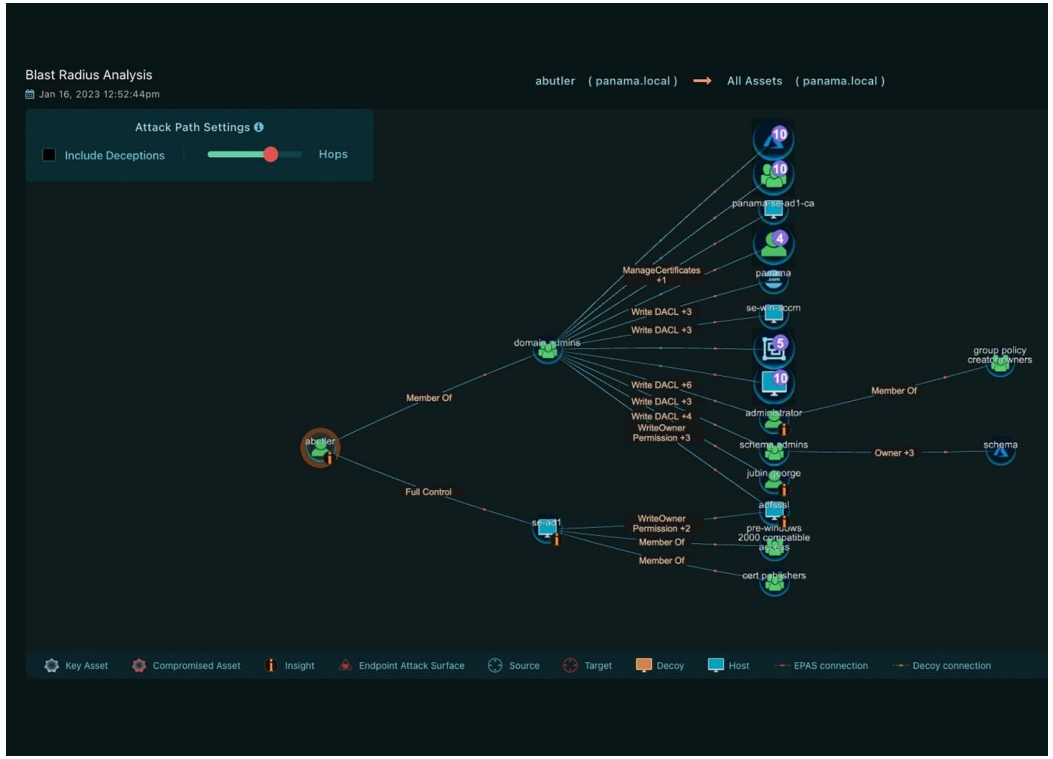
Sestavení klamné platformy

- Automatizované - Sensor provede Discovery, navrhne „Deception playbook“
- Přizpůsobitelné – Deception playbook lze customizovat za hrany strojového učení
- Bezagentské – Nevytěžuje endpointy, využívá stávajících nástrojů (EDR, SDM)
- Dynamické – Přizpůsobí se aktualizacím OS, změnám zařízení



Detect & react

- **Jasné a přesné alerty**
- Vizuální reprezentace nálezů pro rychlé pochopení
- Blast radius analysis
- **Nativní integrace / API umožňují:**
  - Izolaci zařízení
  - Ukončení procesů
  - Vlastní pokročilé reakční scénáře (SOAR)



Souhrn

- Zásadní zkrácení detekčních časů- Ze dnů na minuty
- Rychlá a snadná interpretace nálezů

- Automatizovaný proces nasazení
- Více než 150 různých druhů návnad
- Ochrana „nechránitelných zařízení“

COMGUARD

cyber security masters

Děkujeme za pozornost!