Správa IT infrastruktury:
lépe, snadněji, bezpečněji a levněji

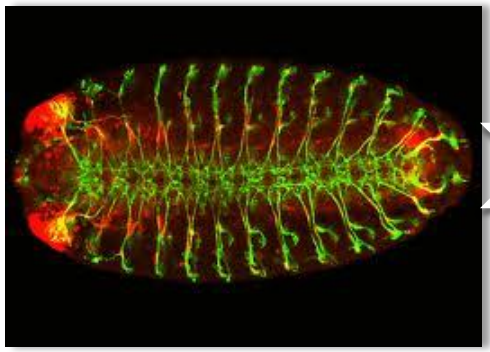
Komplexní řešení pro monitorování a bezpečnost datové sítě

ADVAiCT

Úvod

Bezpečnost IT infrastruktury

	Tradiční metody a přístupy	AdvaICT
Místo instalace	Perimetr	LAN, datové centrum, perimetr
Metoda detekce	Analýza L7, na základě signatur	Analýza L3/L4, statistika, chování
Druh hrozeb	Známé hrozby	Známé L3/L4 a neznámé hrozby
Rozsah	Bezpečnostní hrozby	Bezpečnostní, provozní a výkonnostní problémy

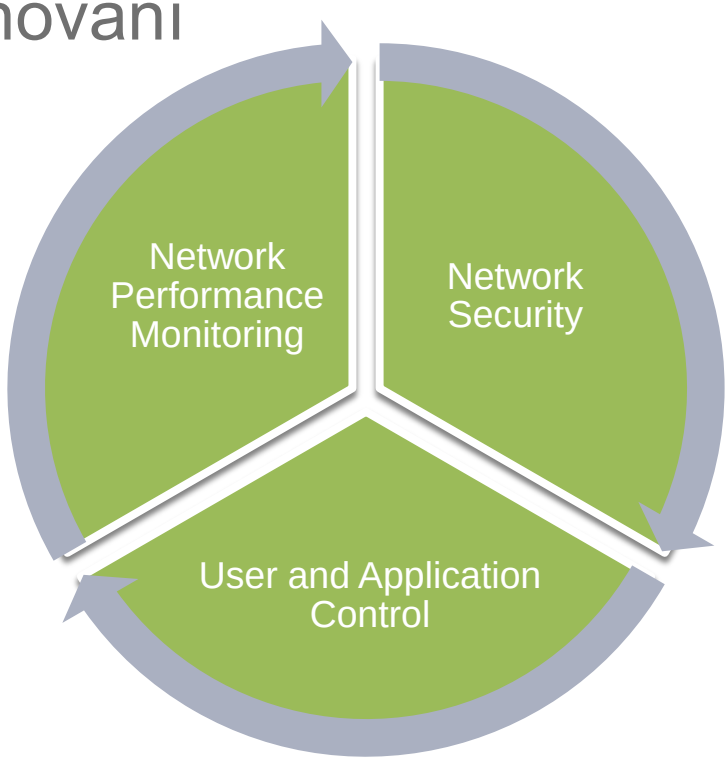


… 2005 2010 2012 …

Řešení AdvaICT

Anomaly Detection System

- Detekce nežádoucích vzorů chování
  - Vnitřní i vnější útoky
  - Známý i neznámý malware
  - Nežádoucí služby a aplikace
  - Provozní a konfigurační problémy
- Behaviorální analýza
  - Profily chování
  - Detekce anomálií
  - Sběr statistik



- Uživatelské rozhraní
  - Dashboard s okamžitou indikací problémů a top statistik
  - Analytické možnosti, interaktivní vizualizace událostí
  - Integrace informací ze služeb DNS, WHOIS, geolokační služby

Historie společnosti

Hlavní milníky

2006 → 2009 → 2010 → 2011 → …

- Založení společnosti týmem z Masarykovy univerzity
- Zahájení vývoje vlastních prototypů
- Validace prototypů s průmyslovými partnery

Historie společnosti

Hlavní milníky

2006 | **2009** | 2010 | 2011 | …

- Uzavřena smlouva o využití výsledků VaV s Masarykovou univerzitou
- Realizován transfer výsledů VaV podložený smlouvou
- Uvedení beta verze produktu
- Vznik obchodního oddělení společnosti

Historie společnosti

Hlavní milníky

- Nasazeno řešení FlowMon ADS u prvního komerčního zákazníka
- Získáno ocenění Inovace roku 2010
- Spuštění on-line služby NetHound
- Do konce roku 2010 získáno 20+ referencí

Historie společnosti

Hlavní milníky

2006 → 2009 → 2010 → **2011** → …

- AdvaICT součástí skupiny Matador Holding
- Expanze na slovenský trh
- Získáno první místo v soutěži IT Produkt roku 2011
- Realizován specifický výzkum na MU pro potřeby AdvaICT
- MU získává první licenční poplatky
- Založena AdvaICT, Inc. se sídlem ve Washingtonu, USA
- Do konce roku 2011 získáno 100+ referencí

Technologie AdvaICT

Rodina produktů AdvaICT


Analýza síťového provozu

Zákazník, a.s.

Anomálie a bezpečnostní rizika

Tato kapitola sumarizuje zjištěné provozní a bezpečnostní problémy a obecné anomálie provozu datové sítě. Hlavní důraz je kladen na odhalení útoků a nežádoucích aktivit na datové síti, které mohou znamenat infikované zařízení nebo úmysl uživatele. Pozornost je rovněž věnována poškozenému provozu s cílem předcházet šíření SPAMu z analyzované sítě.

Útoky

Po dobu monitoringu bylo detekováno několik pokusů o získání neoprávněného přístupu ke službě SSH, tzv. slovníkový útok. Všechny tyto útoky, až na jedinou výjimku, byly neúspěšné a typicky jim předcházel masivní sken sítě. Útoky na protokol Telnet nebyly detekovány. Doporučujeme prověřit útok na IP adresu 10.0.1.96, který byl vyhodnocen jako potenciálně úspěšný. Jednalo se o útok z 2016-07-23 12:26:54 z IP adresy 208.115.230.125.

Nežádoucí aktivity

Mezi běžné nežádoucí aktivity řadíme útoky typu denial of service nebo skenování portů. Vzhledem k otevřenosti sítě jsou zajímavé pouze aktivity, které mají původ v monitorované síti.

IP Address	Nr. of events IP acts as a source	Nr. of events IP acts as a target
10.0.1.10	1	0
10.0.1.70	103	0

Kontakt

AdvaICT, a. s.

Jundrovská 618/31, 624 00 Brno

tel.: +420 511 112 170,

info@advaict.com, **www.advaict.com**

Správa IT infrastruktury:
lépe, snadněji, bezpečněji a levněji