CORTEX XDR

BY PALO ALTO NETWORKS

Detekce, prevence a odezva v síti a na koncových bodech

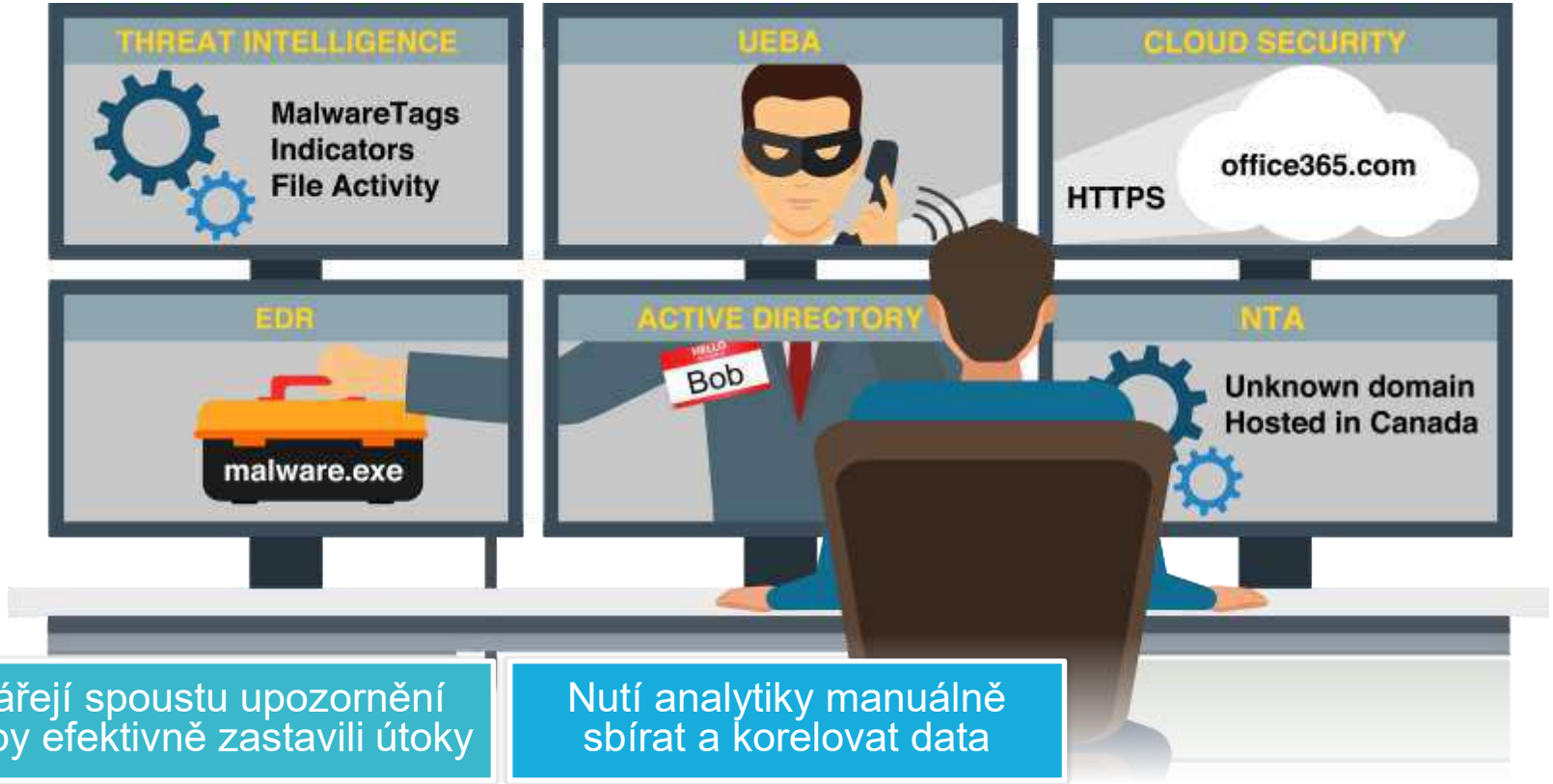
Tibor Tvardzik & Radim Pácl

Palo Alto Networks

SEPERÁTNÍ NÁSTROJE ZPOMALUJÍ VYŠETŘOVÁNÍ A ODEZVU

Vytvářejí spoustu upozornění než aby efektivně zastavili útoky

SEPERÁTNÍ NÁSTROJE ZPOMALUJÍ VYŠETŘOVÁNÍ A ODEZVU



Vytvářejí spoustu upozornění než aby efektivně zastavili útoky

Nutí analytiky manuálně sbírat a korelovat data

SEPERÁTNÍ NÁSTROJE ZPOMALUJÍ VYŠETŘOVÁNÍ A ODEZVU

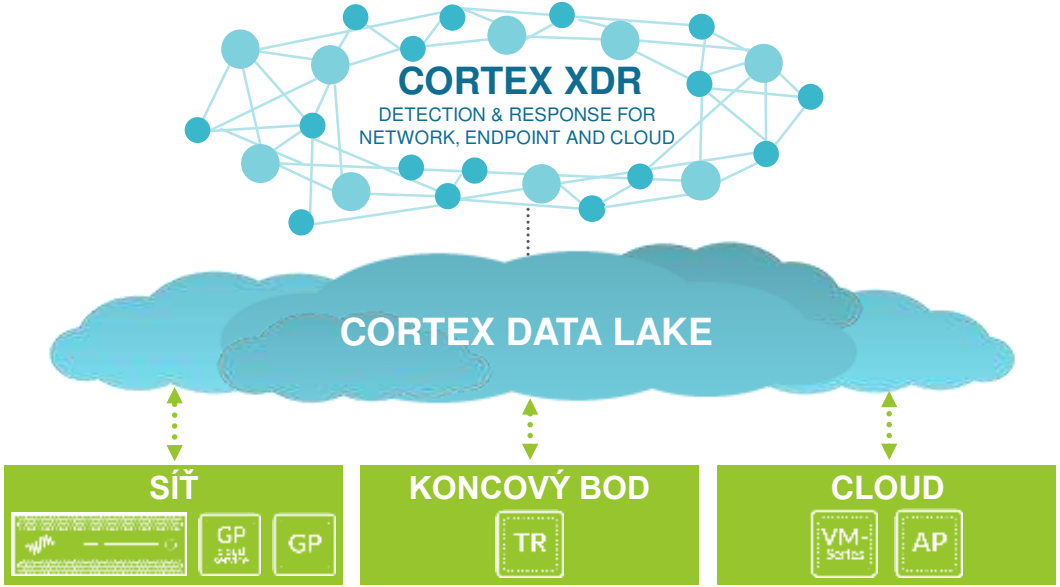
Vytvářejí spoustu upozornění než aby efektivně zastavili útoky

Nutí analytiky manuálně sbírat a korelovat data

Nesbírá všechna potřebná data a vytváří slepá místa

CORTEX XDR: BREAKING SECURITY SILOS

CORTEX XDR: BREAKING SECURITY SILOS



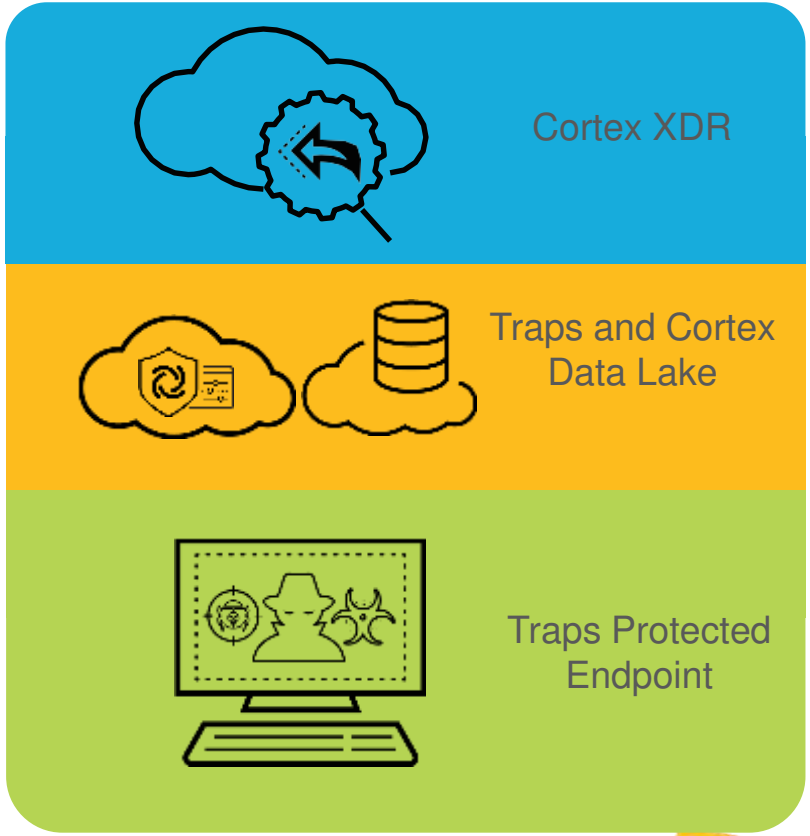
Automaticky detekuje útoky použitím bohatých dat a cloudové behaviorální analýzy

Zrychluje vyšetřování párováním dat pro odhalení příčiny problému

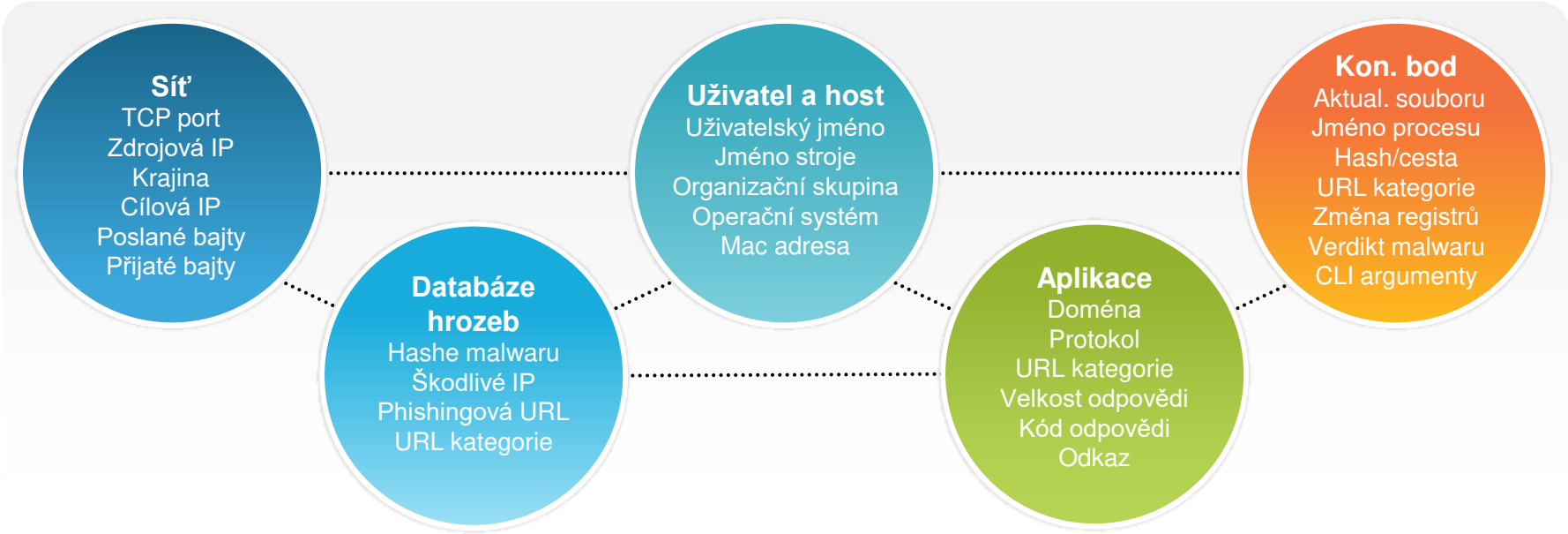
Vysoce integrovaný s platformou pro zastavení hrozeb a přizpůsobení ochrany

BOHATÝ ZBĚR DAT PRO CORTEX XDR

- Posbíraná data slouží pro vyšetřování, vizualizaci a toky detekce
- Kontrolována přes aktualizaci obsahu:
  - Vytvoření/ukončení procesu
  - Modifikace registrů
  - Načítání obrázků
  - Informace o přihlášení/odhlášení
  - Modifikace souboru
  - Síťové relace (5-tuple)
  - Koncové body: změny času a nabootování



KORELOVANÉ DATA Z KONCOVÝCH BODŮ PRO ANALÝZU



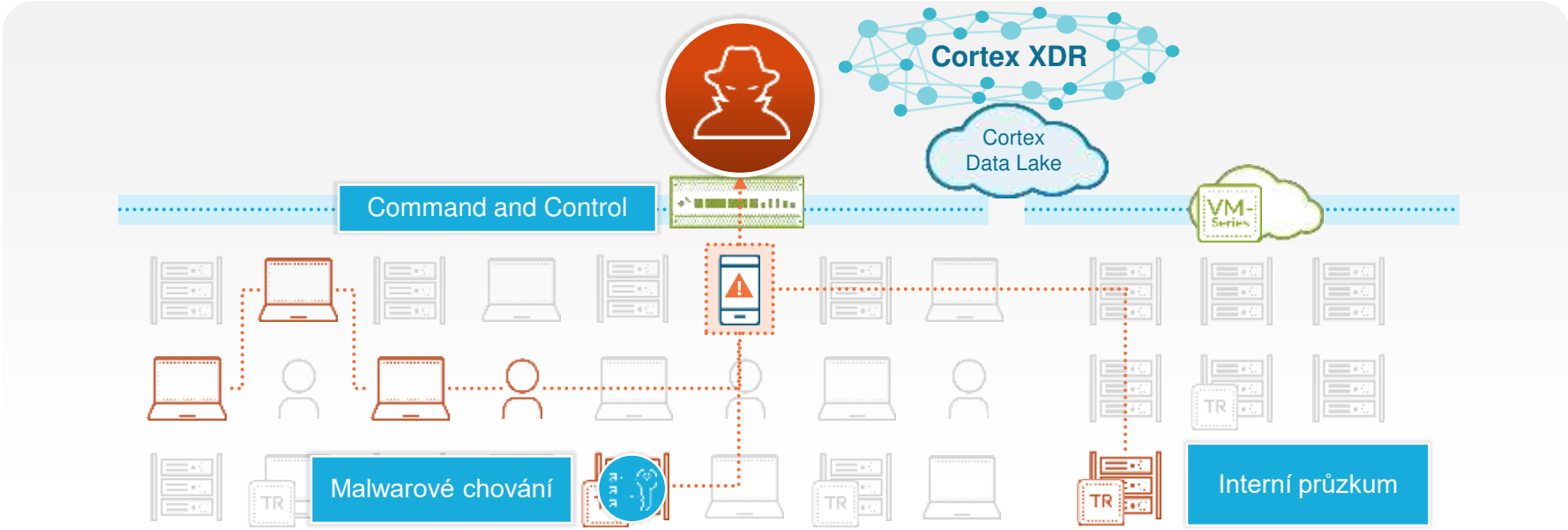
Sbírá bohaté data pro behaviorální analýzu & AI

Automaticky páruje data dohromady pro korelaci aktivit a získání obsahu

PÁRUJE DATA – AUTOMATICKÁ ANALÝZA PŘÍČINY PROBLÉMŮ

1. Vyšetřujte libovolná upozornění jediným klikem
2. Automaticky odhalte příčinu a postupnost událostí
3. Zahrnuje obsah včetně BIOC, databázi hrozeb, časovou os a další detaily

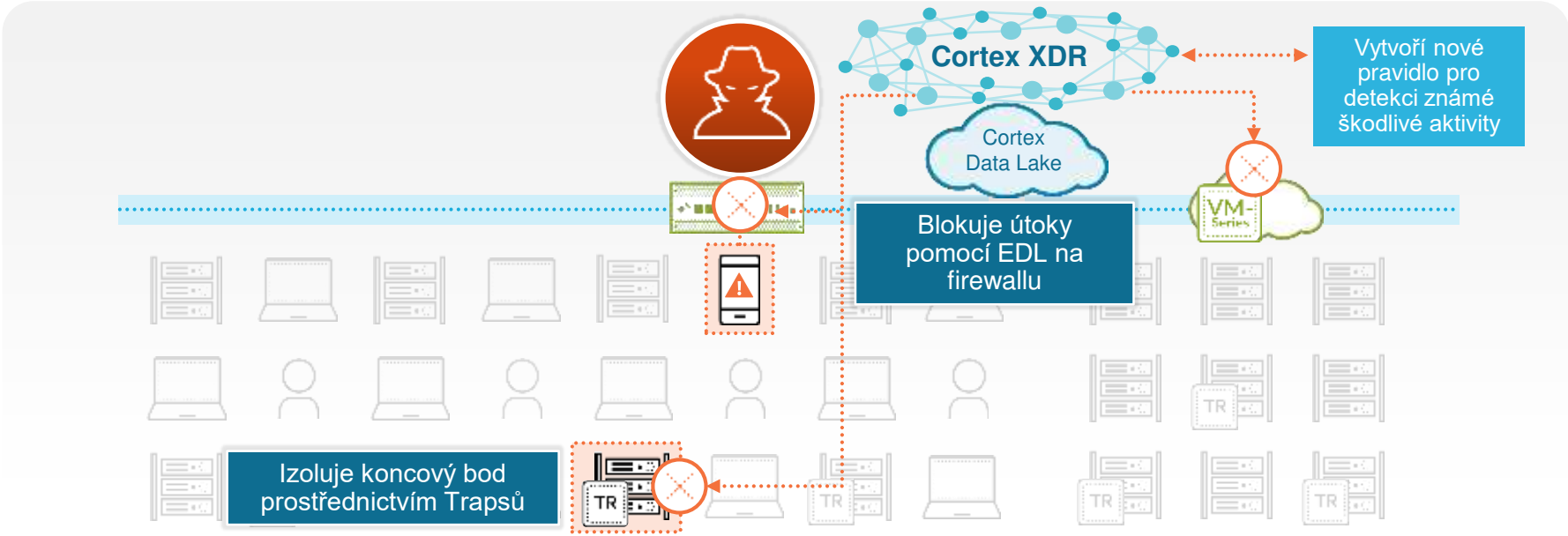
AUTOMATICKY DETEKUJE ÚTOKY BEHAVIORÁLNÍ ANALÝZOU



Útočníci často provádějí tisíce úkonů, přičemž každý z nich může vypadat nevinně

Cortex XDR profiluje chování tak, aby nalezl anomálie indikující útok

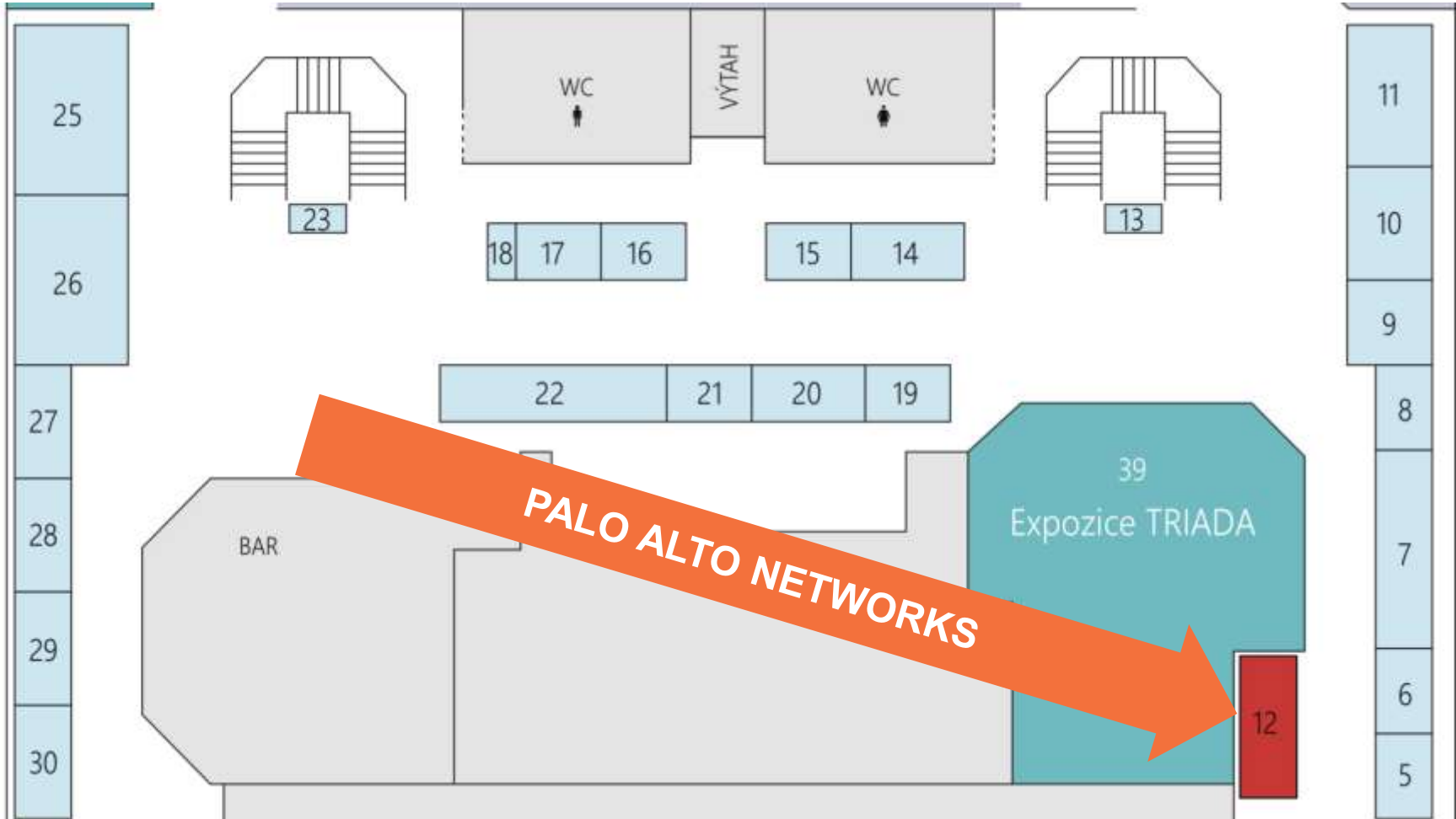
REAKCE A ADAPTACE NA HROZBY



Jednoduše zastaví hrozby úzkou integrací s platformou

Aplikuje získané poznatky pro detekci budoucích hrozeb a zjednodušení vyšetřování

STÁNEK PALO ALTO NETWORKS



DĚKUJEME!

THIS REALLY IS THE END!

