# Bezpečnostní deštník zajišťující orchestraci, automatizaci a reakci na krizové události

IBM SECURITY
—
Adam Muška
Security Presales CZ/SK
adam.muska@ibm.com

# Čím se zabývá IBM Security?

STRATEGIE A RIZIKA

## NASTAVENÍ

- Strategie a plánování
- Hodnocení rizik
- Poradenské služby

DIGITÁLNÍ DŮVĚRA

## OCHRANA

*Ochrana kritických aktiv*

- Data Protection Services
- Guardium
- Data Risk Manager
- Multi-cloud Encryption
- Key Lifecycle Manager

*Digitální identita*

- Trusteer
- Verify

*Uživatelé a identity*

- Identity Management Services
- Identity Governance
- Verify
- Verify Access
- Secret Server

*Správa koncových bodů*

- Endpoint Management Services
- MaaS360

SPRÁVA KYBERNETICKÝCH HROZEB

## SPRÁVA

***Zastavení pokročilých hrozeb***

- Security Operations Consulting
- X-Force Threat Management Services
- X-Force Red
- QRadar

***Orchestrate Incident Response***

- Resilient
- X-Force IRIS

***Master Threat Hunting***

- i2 Intelligence Analysis
- QRadar Advisor with Watson

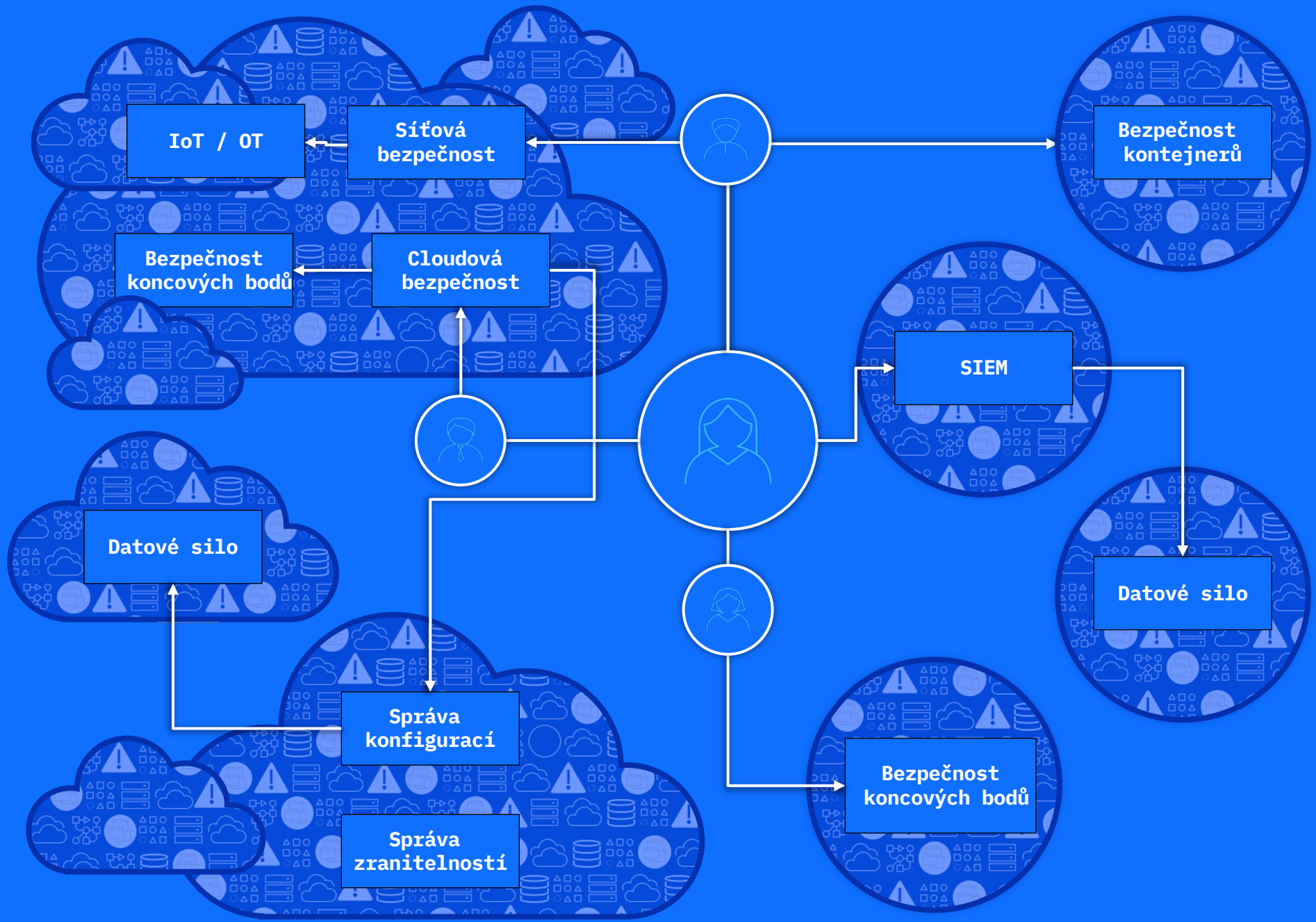
## MODERNIZACE

Cloud Pak for Security | Cloud Security Services | Cloud Security Products

# Mnoho hrozeb, nástrojů a dat

## Bezpečnostní analytici potřebují pomoc...

- Prioritizovat zvyšující se množství událostí, poplachů a informací, které mají k dispozici
- Rychle prohledávat mnoho odlišných bezpečnostních nástrojů
- Se snížením počtu manuálních procesů



# Zajištění bezpečnosti na všech úrovních

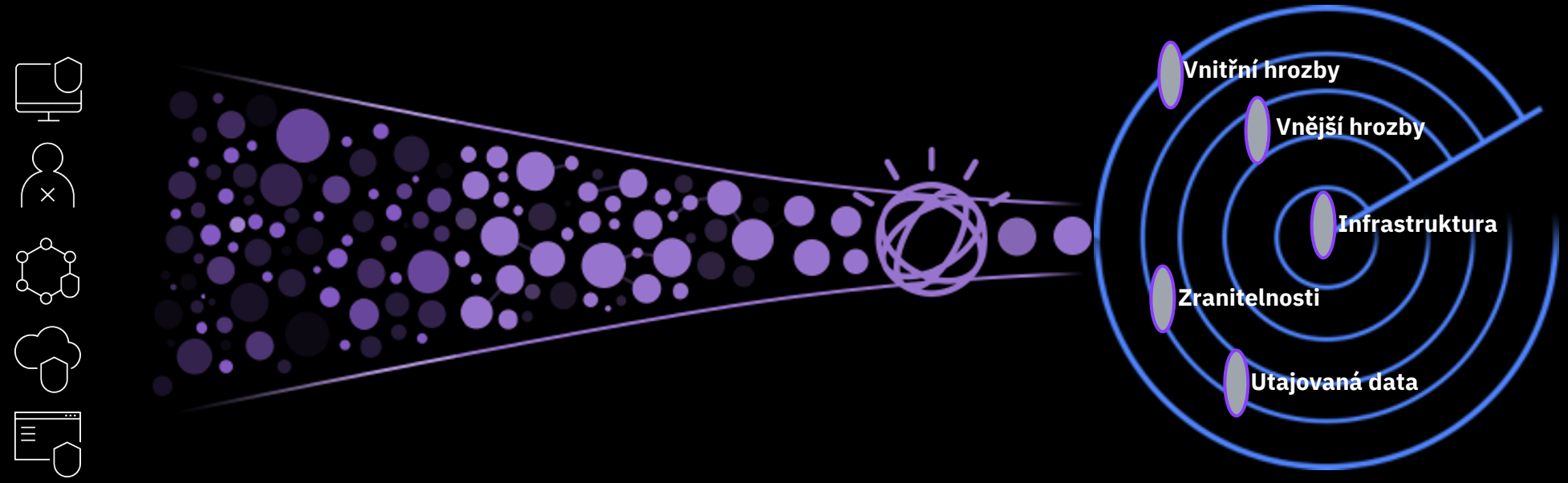
IBM **Security**

## Viditelnost

## Detekce

## Vyšetřování

## Reakce




Sběr dat

Normalizace dat

Bezpečnostní incidenty

Dopady a vizualizace incidentů

Pracovní postupy nápravná opatření

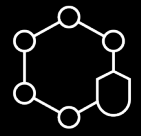
# 4 pilíře efektivní správy hrozeb

IBM **Security**

## Viditelnost

- Normalizace
- Kategorizace
- Obohacení dat
- Síť, stanice, server, cloud, uživatel a aplikace

## Detekce



- MITRE ATT&CK
- Modely chování
- Vzájemná korelace dat
- Globální informace o hrozbách
- X-Force

## Vyšetřování

- AI
- Analýza spojení
- Data mining
- Učící algoritmy
- Analýza nestrukturovaných dat
- Federované vyhledávání

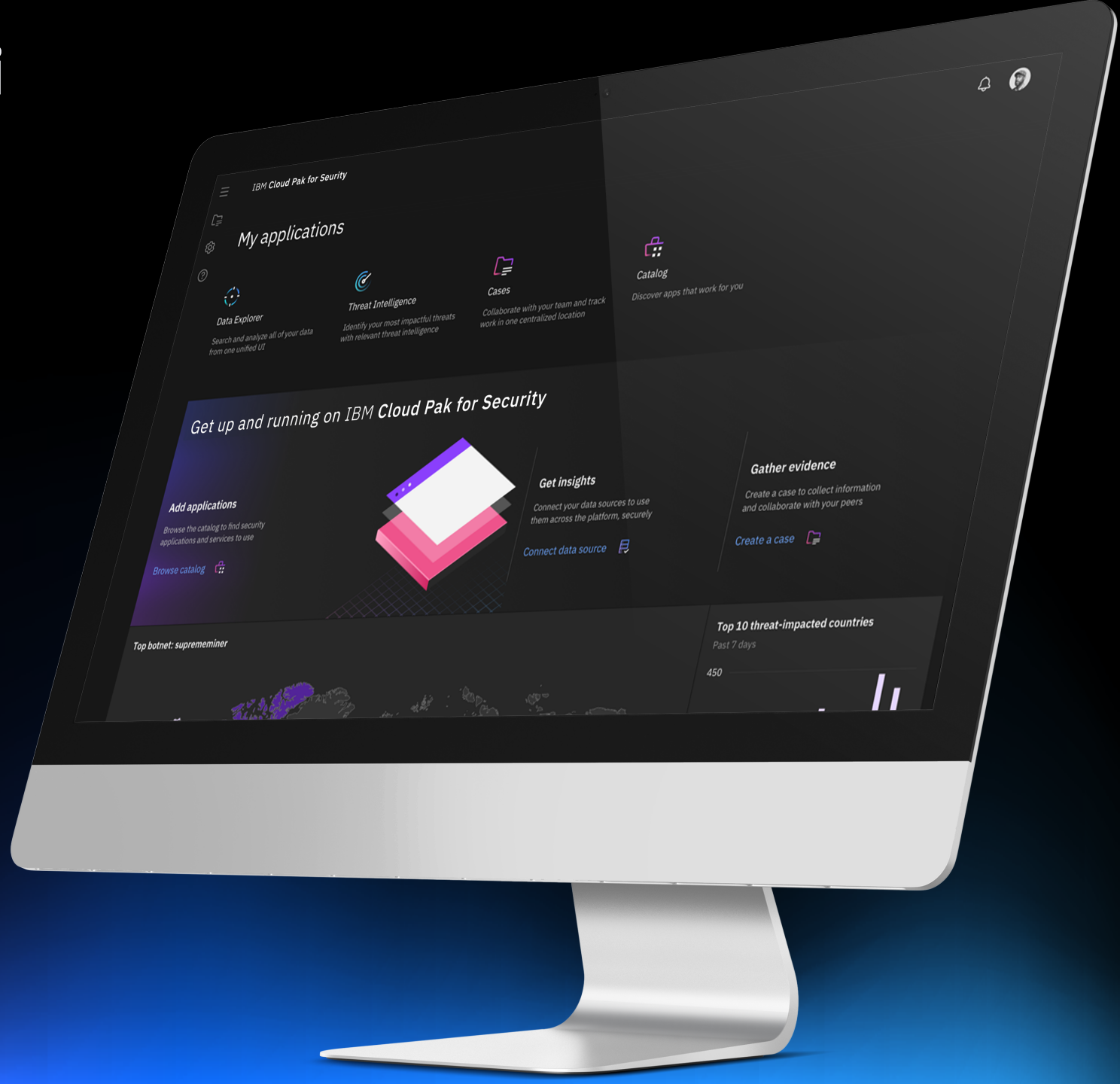
## Reakce

- Dynamické workflow
- Automatizace
- Orchestrace
- Reporty o únicích dat

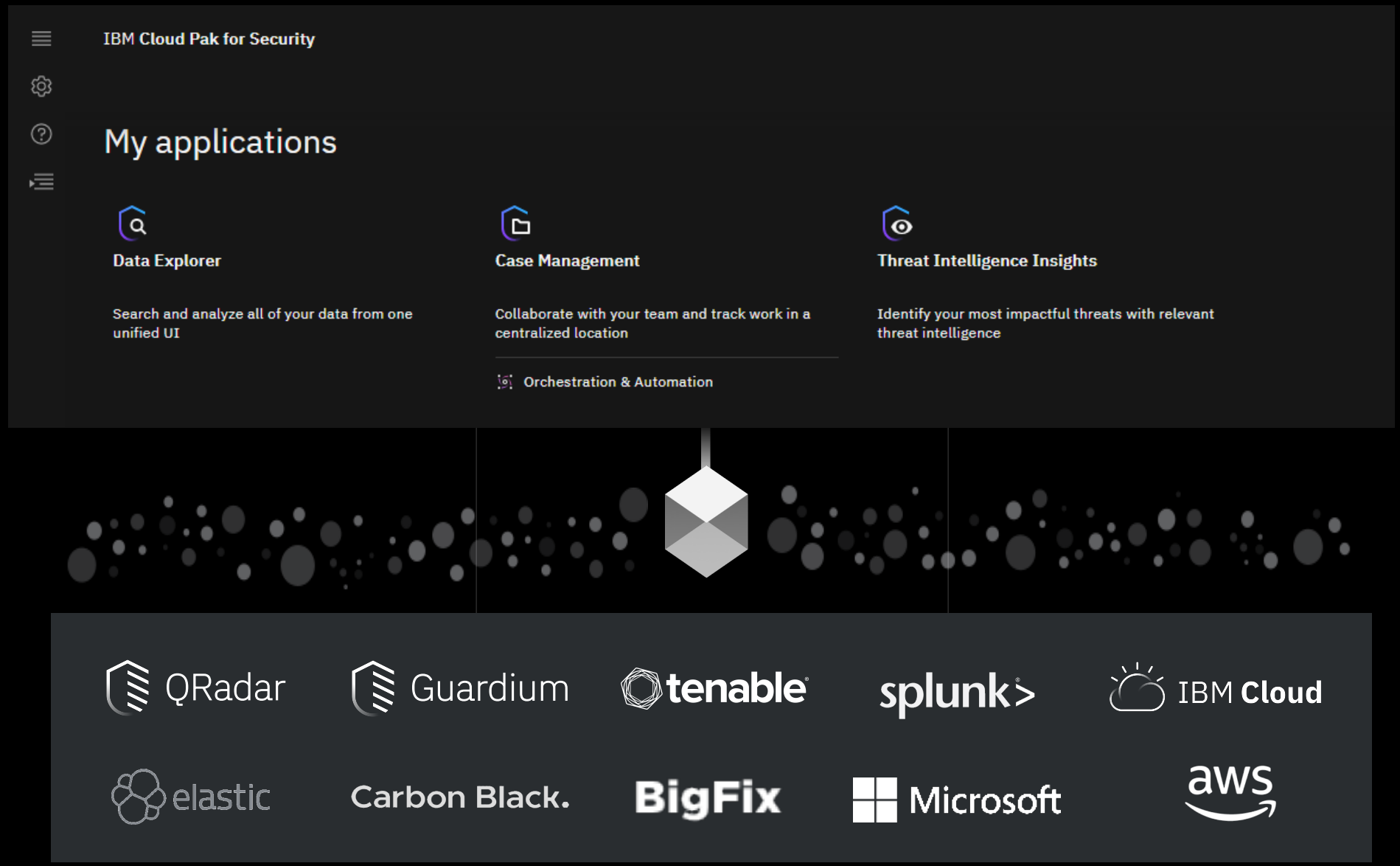
# Modernizace bezpečnosti

## Integrovali jsme všechny klíčové bezpečnostní řešení do Cloud Pak for Security

- Běží na kontejnerizační platformě RedHat Openshift - on premise nasazení k dispozici
- Bezpečnostní vhledy do dat bez nutnosti je přesouvat
- Rychlejší reakce na incidenty díky automatizaci



# Cloud Pak for Security dokáže integrovat mnoho vašich již existujících bezpečnostních řešení - Agregační vrstva pro všechny vaše data bez nutnosti jejich přesunu



# Demo Ukázka

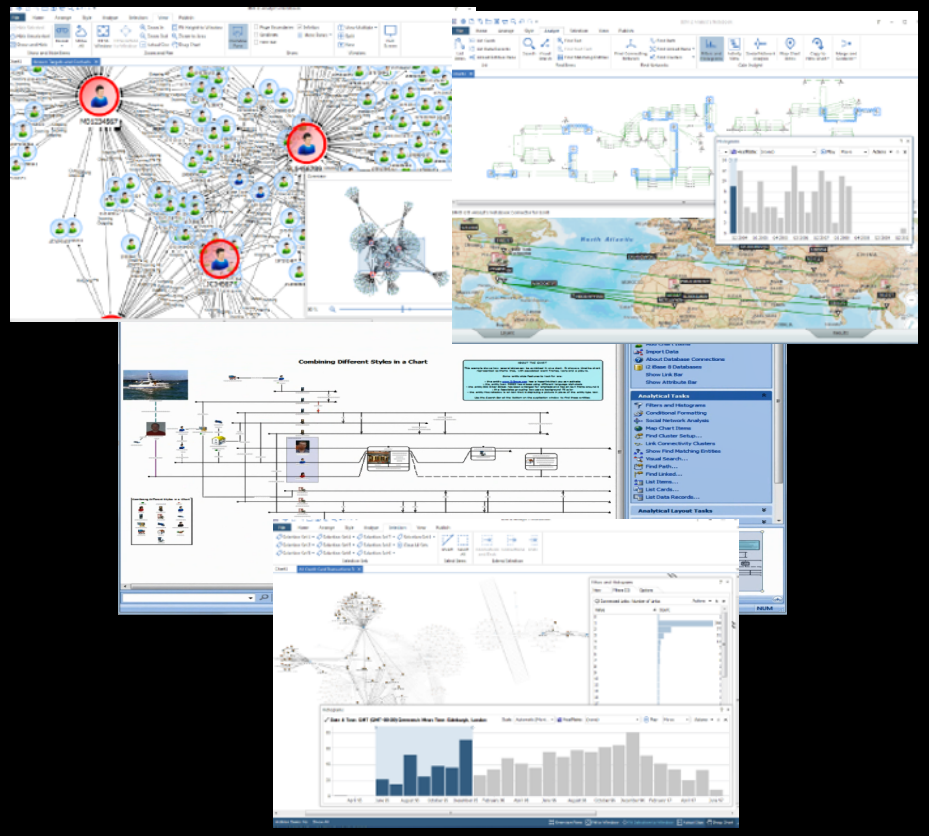
URL odkaz: https://www.youtube.com/watch?v=fChSxLCd6kg

# IBM i2

## Podpora analytických činností

- propracované vizualizace
- mapové podklady, síťové grafy
- textová analýza
- statistické modely
- konektory pro jakákoli data

...



1990 i2 založeno v Cambridge, UK

2011 akvizice IBM

aktuálně více než 4000 zákazníků

zákazníci ve více než 100 zemích po celém světě

nasazené prakticky ve všech průmyslových odvětvích

**i2 Analyst Notebook**
tradiční desktopový nástroj pro analytiky

**i2 Connect**
otevřené konektory pro jakékoli datové zdroje (strukturované i nestrukturované)

**i2 Enterprise Insight Analysis**
serverová platforma s řízením přístupu k datům, vlastním optimalizovaným datovým úložištěm, tenkým klientem a řadou dalších funkcí..

# Děkuji za pozornost