

Bezpečnostní monitoring a vyšetřování v hybridní multicloud infrastruktuře

Adam Muška

Client Technical Specialist

adam.muska@ibm.com

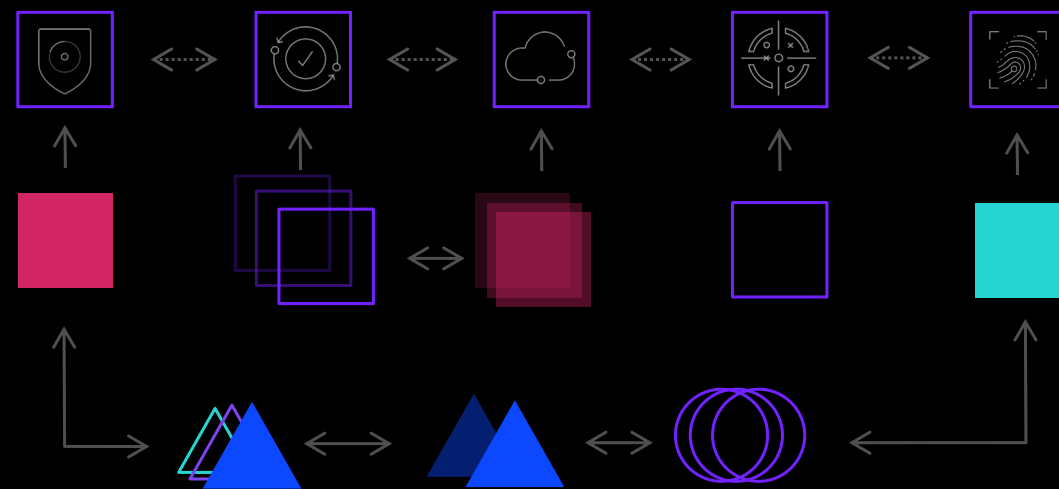
IBM Cloud / IBM Klientské centrum/ 14. března 2019/ © 2019 IBM Corporation



Bezpečnost je fragmentovaná, oddělená a komplikovaná kvůli multicloudu



Co když by byla
bezpečnost
sjednocená,
propojená?



Získat bezpečnostní
vhledy

Propojení
dat

Reagovat rychleji

Propojení
workflow

Spustit kdekoliv

Otevřená
platforma

Získat bezpečnostní
vhledy

Propojení dat

- Odhalte skryté hrozby
- Provádějte kvalitnější rozhodnutí na základě rizika
- Nechte vaše data tam kde jsou
- Získejte více z vašich investic

Reagovat rychleji

Propojení workflow

- Reagujte rychleji jako tým
- Organizujte napříč bezpečnostními use cases
- Snižte náklady na integraci řešení
- Rozšiřte schopnosti vašeho bezpečnostního týmu

Spustit kdekoliv

Otevřená platforma

- Operujte v on-premise, privátním cloudu nebo veřejném cloudu
- Zvyšte a nasměrujte investice jak je potřeba
- Nebudte závislí na výrobci
- Podporujte vzájemnou spolupráci bezpečnostních nástrojů

Open Cybersecurity Alliance (OCA): Aliance spoluzaložená IBM k propagaci a podpoře otevřené bezpečnosti

Kdo

Globální stejně smýšlející výrobci, koncoví uživatelé, osobnosti v oblasti kybernetické bezpečnosti

Vize

Otevřený ekosystém kybernetické bezpečnosti:
Produkty si navzájem zdarma vyměňují informace, vhledy, analytiku a organizují nápravné opatření

Jak

Otevřený
vývoj kódu & nástrojů
Otevřená shoda na používaných
technologiích, standardech a postupech



Původně zapojené projekty – Stix Shifter a Open DXL Ontology na Github platformě

Zapojení v OCA – původní počet členů se navýšil z 16 na 27

IBM Cloud Pak for Security

Platforma, která rychleji integruje vaše existující bezpečnostní nástroje a dokáže generovat hlubší vhledy do aktuálních hrozeb, organizovat akce a automatizovat nápravná opatření na vzniklé hrozby — vše s tím, že nechává data na původním místě.

- Hybridní, multicloud architektura
- Propojený, otevřený ekosystém
- Automatizace a orchestrace



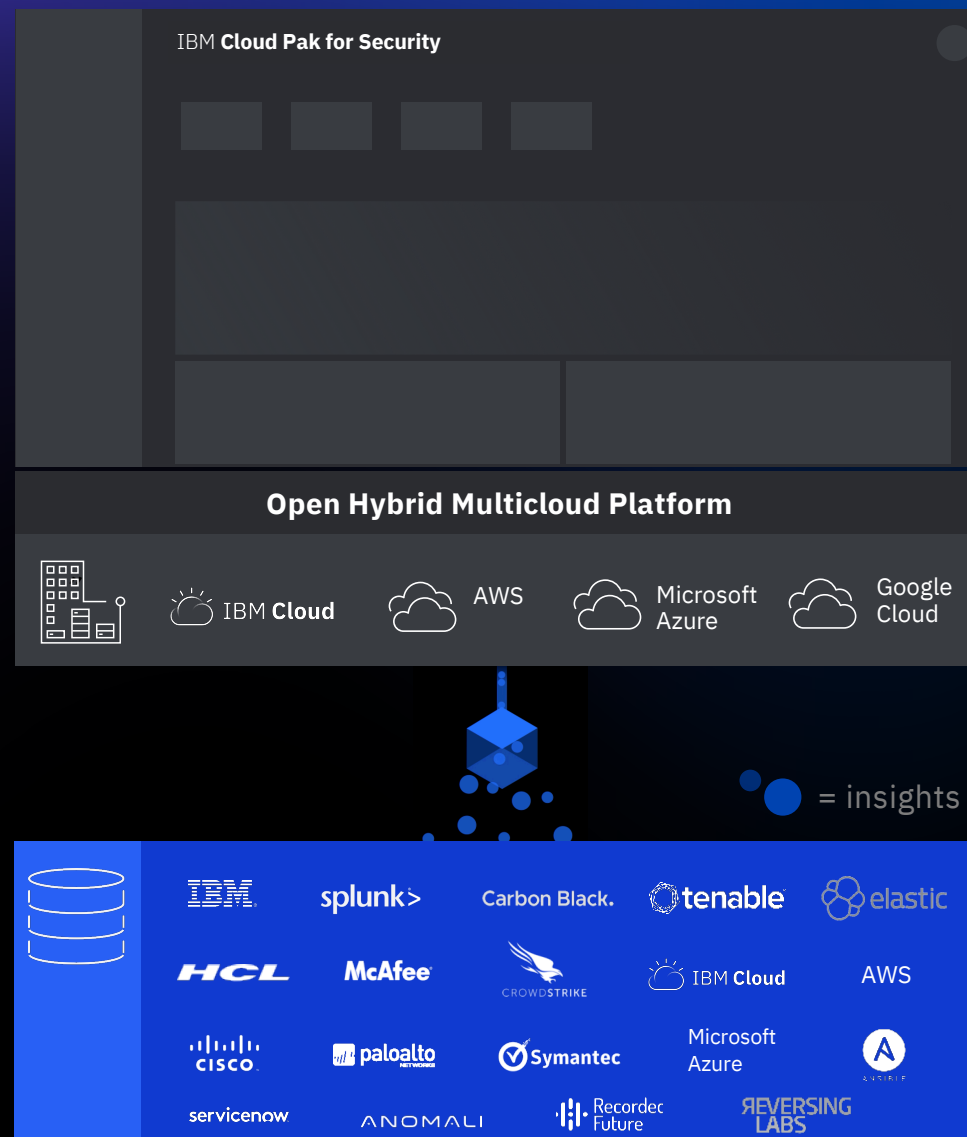
Sjednocené datové vhledy

Získejte kompletní vhled do bezpečnostních událostí bez nutnosti přemísťovat vaše data

Otevřený partner

Bezpečně integrujte nástroje třetích stran v existující bezpečnostní infrastruktuře

IBM Security



Hybridní, multicloud platforma

Moderní, otevřená architektura pro veřejný, privátní, hybridní cloud, s možností nasadit a spustit kdekoliv

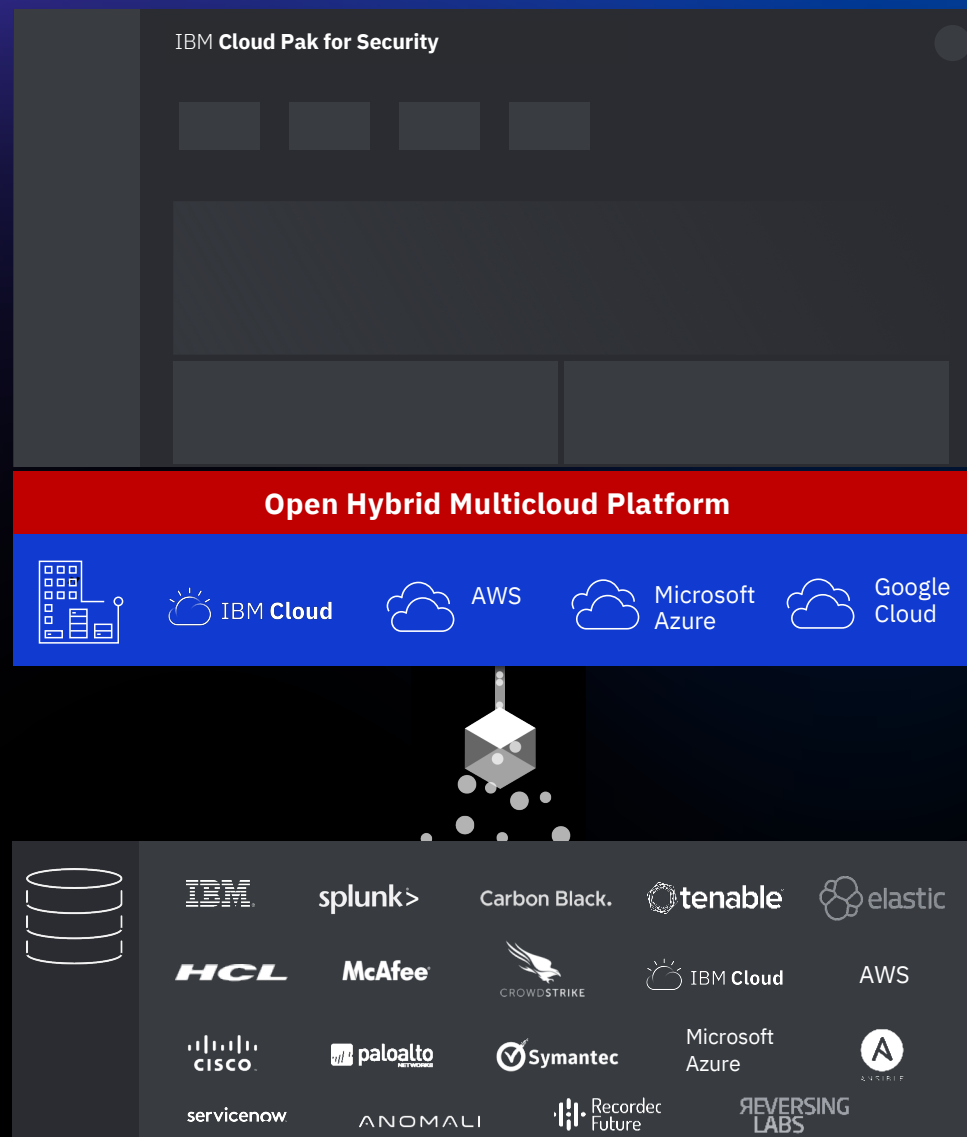
Sjednocené datové vhledy

Získejte kompletní vhled do bezpečnostních událostí bez nutnosti přemísťovat vaše data

Otevřený partner ekosystém

Bezpečně integrujte nástroje třetích stran v existující bezpečnostní infrastruktuře

IBM Security



Jednotné rozhraní a navržený systém

Pracujte napříč jednotným rozhraním, nižší náklady na školení, rychleji stavte aplikace

Řešení zaměřené na výsledek

Out-of-the-box schopnost adresovat bezpečnostní workflow, podpořená orchestrací a automatizací

Hybridní, multicloud platforma

Moderní, otevřená architektura pro veřejný, privátní, hybridní cloud, s možností nasadit a spustit kdekoli

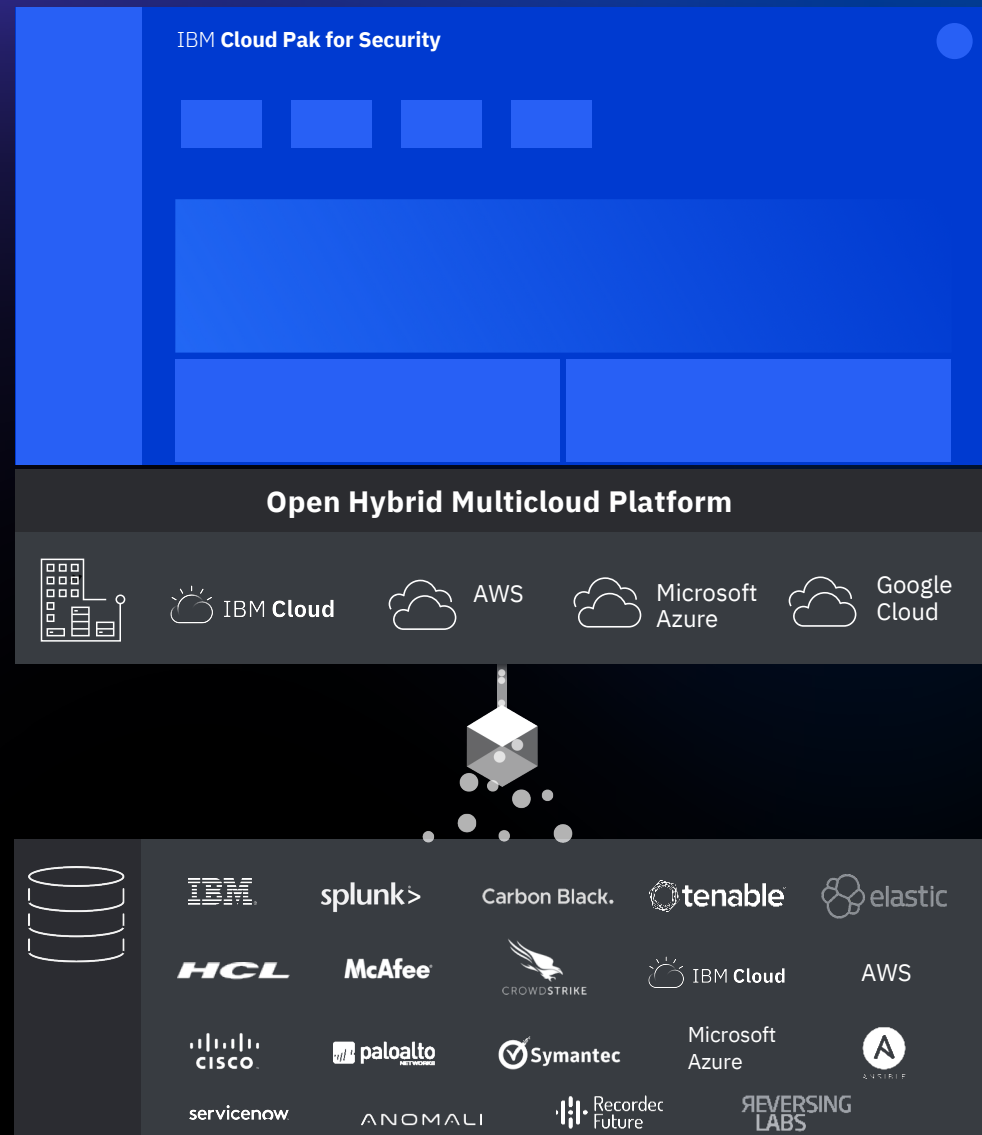
Sjednocené datové vhledy

Získejte kompletní vhled do bezpečnostních událostí bez nutnosti přemísťovat vaše data

Otevřený partner

Bezpečně integrujte nástroje třetích stran v existující bezpečnostní infrastrukturu

IBM Security



IBM Cloud Pak for Security

Bezpečnostní schopnosti

Služby platformy v jádru

Hybridní multicloud architektura

Otevřená integrace s existujícími bezpečnostními nástroji a datovými zdroji

Bezpečnostní vhledy

Reagujte rychleji

Spusťte kdekoliv

Sjednocené bezpečnostní pracovní postupy

Threat Intelligence Insights:
Informace o nových hrozbách a útocích

Data Explorer:
Federované vyhledávání pro vyšetřování

Resilient*:
Reakce na incidenty a týmová spolupráce

Universal data insights

Security orchestration & automation

Development framework

Open Hybrid Multicloud Platform



IBM Cloud



AWS



Microsoft
Azure



Google
Cloud



QRadar



Guardium



tenable

splunk>



IBM Cloud



elastic

Carbon Black.

BigFix



Microsoft



aws

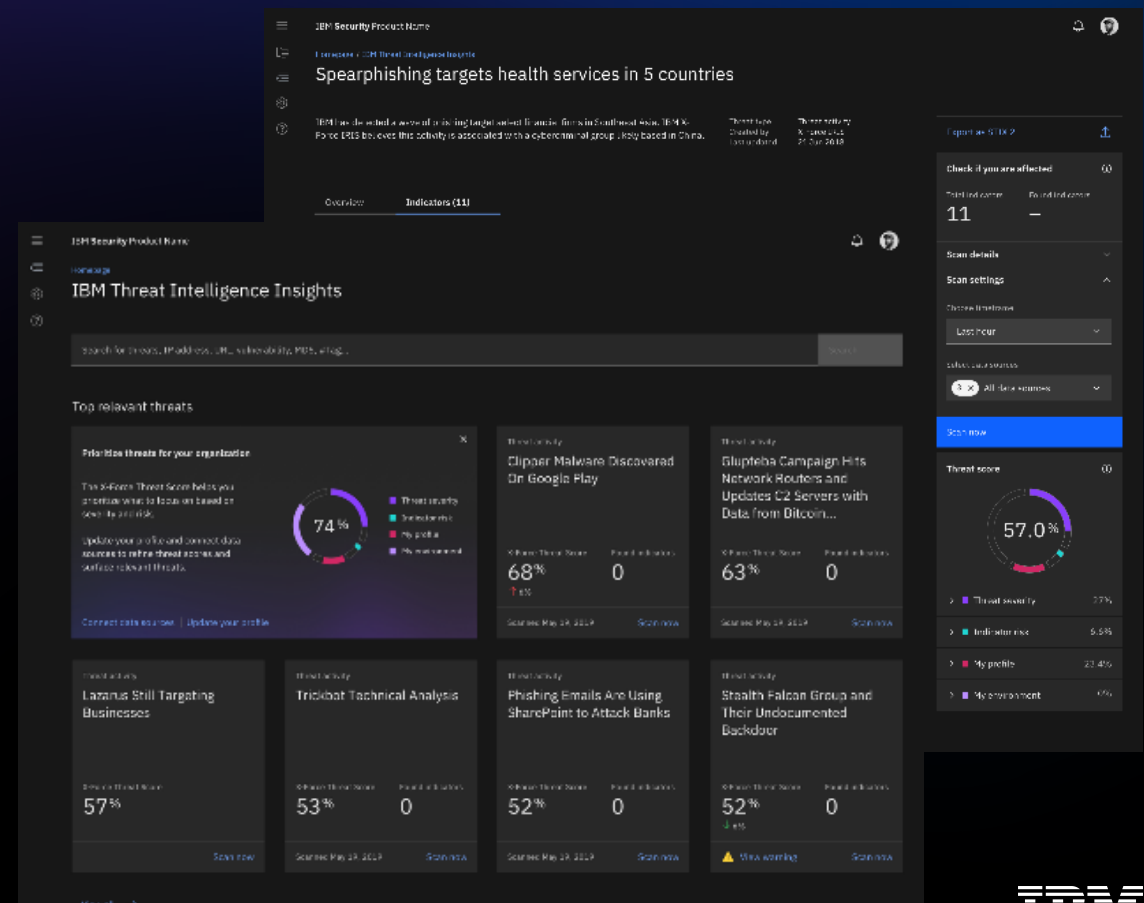
Threat Intelligence Insights

Prioritizované, zpravodajské informace o

hrozbách

- Jednotlivé díky nových informacích o hrozbách s pomocí reportů X-Force Premium Threat Intelligence, které poskytují kontextuální informace díky IBM X-Force IRIS bezpečnostního týmu

- Prioritizujte hrozby díky skóre X-Force Threat, adaptivní hodnotě, vypočtené na základě relevance dané hrozby, závažnosti, penetrace, dopadu a aktuálním pozorováním v prostředí
- Identifikujte hrozby aktivní ve vašem prostředí s pomocí akce „Jsem infikován“, která konstantně spouští a automatizuje hledání přes všechny napojené datové zdroje.
- Pracujte z jediné konzole správy a vyšetřujte hrozby a indikátory kompromitování (IOC) jednoduše napříč vícero řešeními a zneškodněte kybernetické hrozby



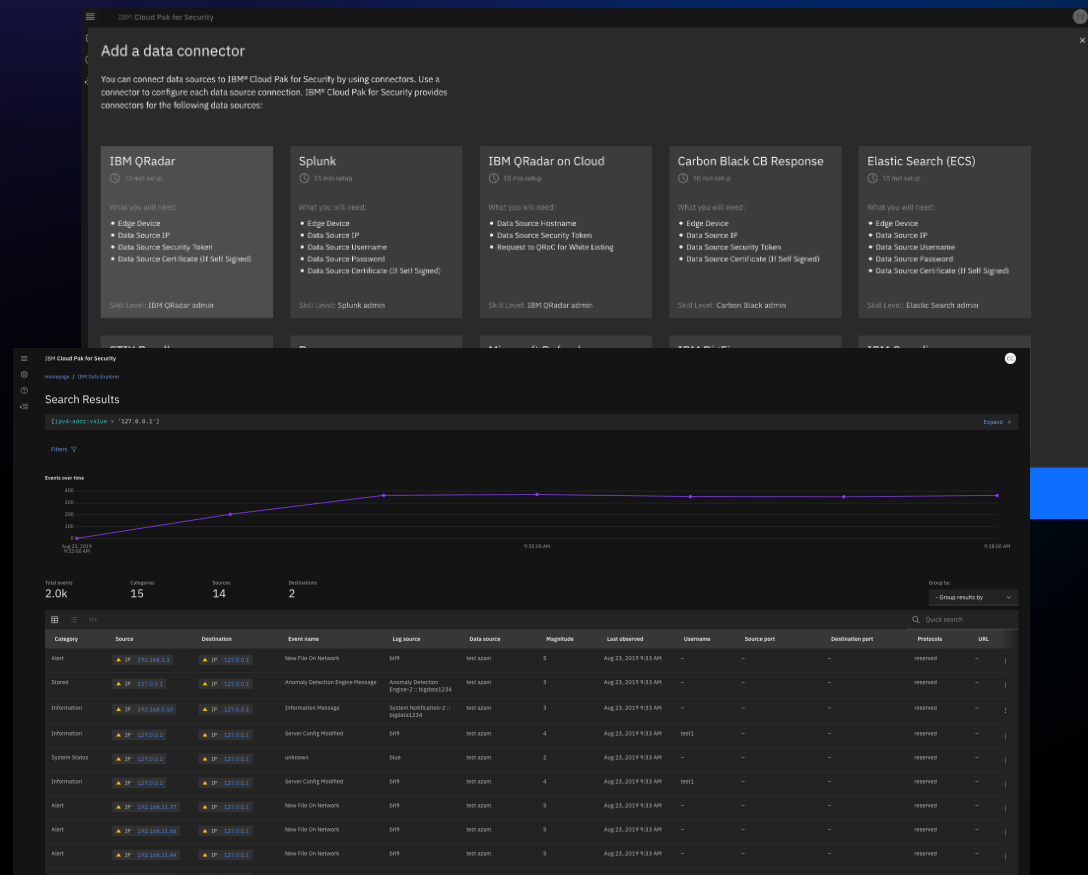
IBM Security



Data Explorer

Federované vyhledávání a vyšetřování

- Napojte vaše kritická bezpečnostní data pomocí konektorů na cloud a bezpečnostní datové zdroje, bez nutnosti přesunu dat samotných
- Spouštějte dotazy na více datových zdrojů najednou bez nutnosti přesouvat data samotná
- Vyšetřujte z jednoho sjednoceného rozhraní pro nalezení hrozeb a IOC
- Naleznete vhledy do bezpečnosti s výkonným vyhledávacím enginem napříč všemi napojenými daty, bez nutnosti přesunu dat samotných
- Sledujte průběh vyšetřování s nástrojem pro správu případů
- Rozšiřte zdroje dat a schopnosti díky SDK nebo IBM služeb a jednoduše napojte další a další data



Resilient

Reakce na incidenty

- Snižte čas potřebný k reakci a nápravě komplexních kybernetických útoků pomocí automatizace IR procesů
- Organizujte a automatizujte manuální a opakující se úkoly jako je např. obohacení IOC o nové data
- Řiďte a zahajujte vyšetřování a reakční akce konzistentně pomocí robustní správy případů a úkolů
- Prioritizujte pracovní zátěž analytiků na závažnější vyšetřování a stanovte postupy pro jejich způsob vyšetřování a reakce
- Zrychlete vyšetřování napříč organizací pomocí rozsáhlé podpory aplikací třetích stran a integrace
- Využijte modelovací nástroj pro jednoduchý návrh postupů při vyšetřování kybernetických incidentů

The screenshot displays the 'Fake AppleID Phishing Email' incident details in the Resilient console. The interface includes a top navigation bar with tabs like Tasks, Details, Breach, Notes, Members, News Feed, Attachments, Stats, Timeline, Artifacts, and Email. The 'Details' tab is active, showing a description: 'This has fooled a number of employees because it looks so real!'. Below this, the 'Basic Details' section lists fields such as Name, Description, Incident Type (Malware Phishing), NIST Attack Vectors (E-mail), Incident Disposition (Confirmed), Phase (Engage), Resolution, and Resolution Summary. The 'Date and Location' section shows the incident was created on 10/03/2019 at 20:13, discovered on 10/03/2019 at 20:12:25, and the owner is Muddy Admin. On the right, a 'Summary' section provides a high-level overview, including the ID (2095), Phase (Engage), Severity (Low), and Date Created (10/03/2019). The 'People' section lists the creator (Muddy Admin) and members (Muddy Admin). The 'Related Incidents' section indicates no related incidents are found.

The screenshot shows the 'Activity Dashboard' in the Resilient console. It features a 'News Feed' section with a timeline of recent actions. The actions include: 'Muddy Admin wrote a note on the incident Fake AppleID Phishing Email' (2 minutes ago), 'Muddy Admin modified the incident Fake AppleID Phishing Email' (4 minutes ago), 'Muddy Admin updated the task list on the incident Fake AppleID Phishing Email' (5 minutes ago), and 'Muddy Admin created the incident Fake AppleID Phishing Email' (5 minutes ago). The 'Show Types' dropdown is set to 'All'. On the right, the 'Tasks Due Soon' section indicates 'You have no tasks due soon.' Below this, the 'Need Help?' section provides links to 'Documentation' and 'Resource Library'. The bottom of the dashboard shows the copyright notice: '© Copyright IBM Corporation 2019'.

Budoucnost je otevřená

Postaveno otevřeně

- Otevřený ekosystém a datové konektory
- Open Source iniciativa
- OASIS Open Cybersecurity Alliance

Chytrá bezpečnost, pro zákaznická

Podpořeno experty v oboru

- Vývoj konektorů pro napojení dat
- Pomoc expertů na požádání
- Komplexní strategické poradenství

