OCHRANA ZÁLOHOVANÝCH DAT PŘED RANSOMWARE

Ing. Ladislav Helcl
Solution Architekt, S&T CZ

PŘEDSTAVENÍ S&T CZ

Partner s přidanou hodnotou

Poskytovatel ICT služeb s přidanou hodnotou a integrací pro finanční sektor, výrobu, utility/telco, retail a státní správu.

S&T group

Sídlo v Rakousku
32 zemí
6000 zaměstnanců

Ing. Ladislav Helcl

- ČVUT FEL
- 10+ let Solutions Architekt v S&T pro oblast datových center
- 20+ let praxe v Mission Critical IT

- S&T CZ založeno v roce 1991
- S&T CZ sídlo Praha
  7 poboček v ČR
- 6 servisních míst
- Cca 300 zaměstnanců v ČR

S&T CZ – PORTFOLIO ŘEŠENÍ, PRODUKTŮ A SLUŽEB

Klíčové oblasti

ERP

PRŮMYSL 4.0 DIGITALIZACE/IOT

APLIKAČNÍ VÝVOJ

DIGITAL. CLOUD

INFRASTRUKTURA

EUS PODPORA

BEZPEČNOST

SAP

ŘÍZENÍ VÝROBY

ODVOD VÝROBY

ATHENA

AZURE/ MICROSOFT 365

VIRTUALIZACE

DATA LIFECYCLE

SERVCE DESK

SOC

END POINT PROTECTION

INFOR

SBĚR DAT

ŘÍZENÍ KVALITY

ZAKÁZKOVÝ SW

D

PODPORA KONCOVÝCH ZAŘÍZENÍ

SIEM

PIM/PAM

IOT

AUTO IDENTIFIKACE

LAN/WAN INFRA

MOBILE SOLUTION

MANAGED PRINT SERVICES

PERIMETR PROTECTION

BC/DR
Business Continuity Disaster Recovery

RANSOMWARE – SOFTWARE PRO VÝKUPNÉ

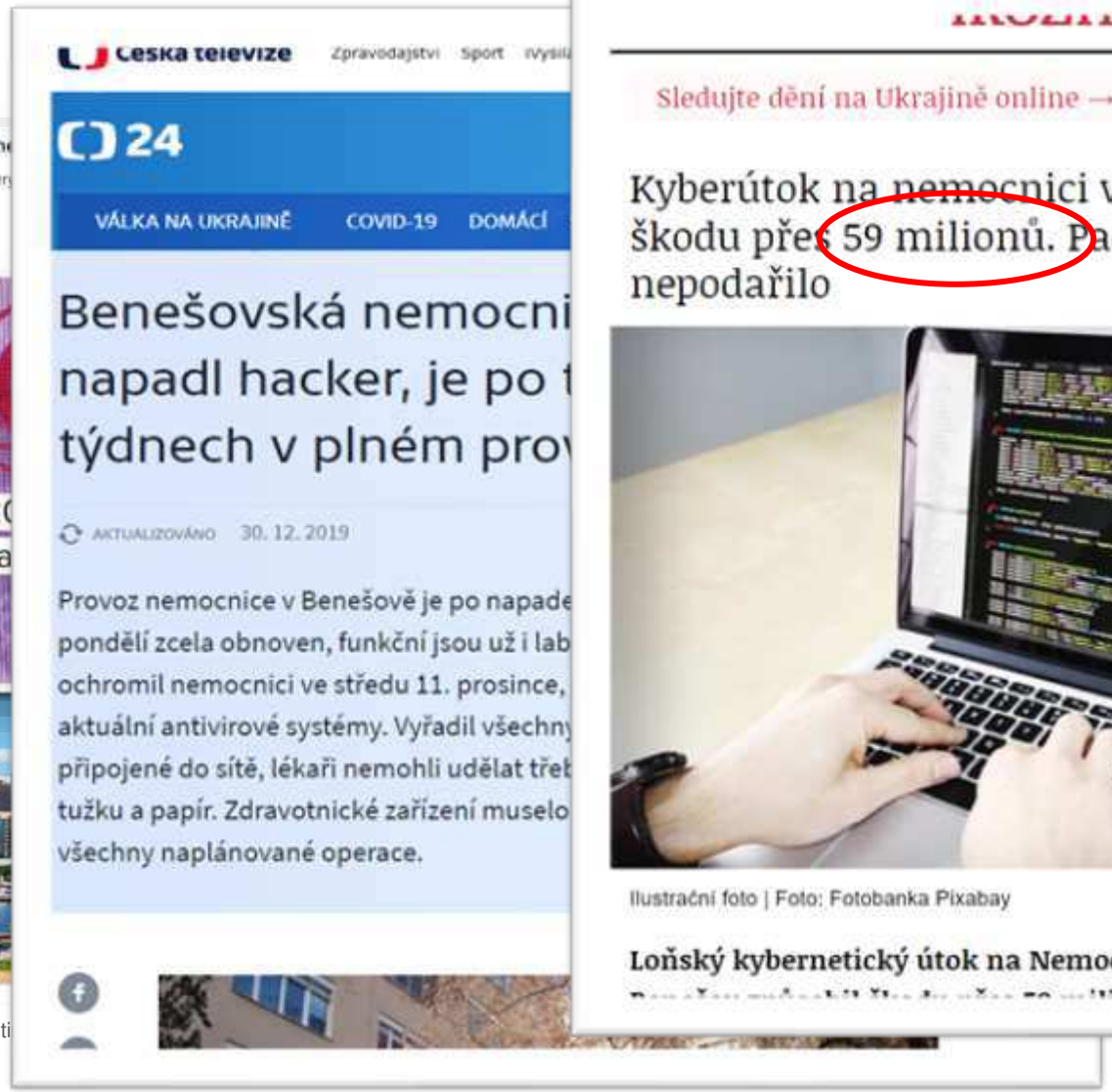
Kdo z vás se již setkal s útokem ransomware?

KYBERÚTOKY JSOU KAŽDODENNÍ REALITA

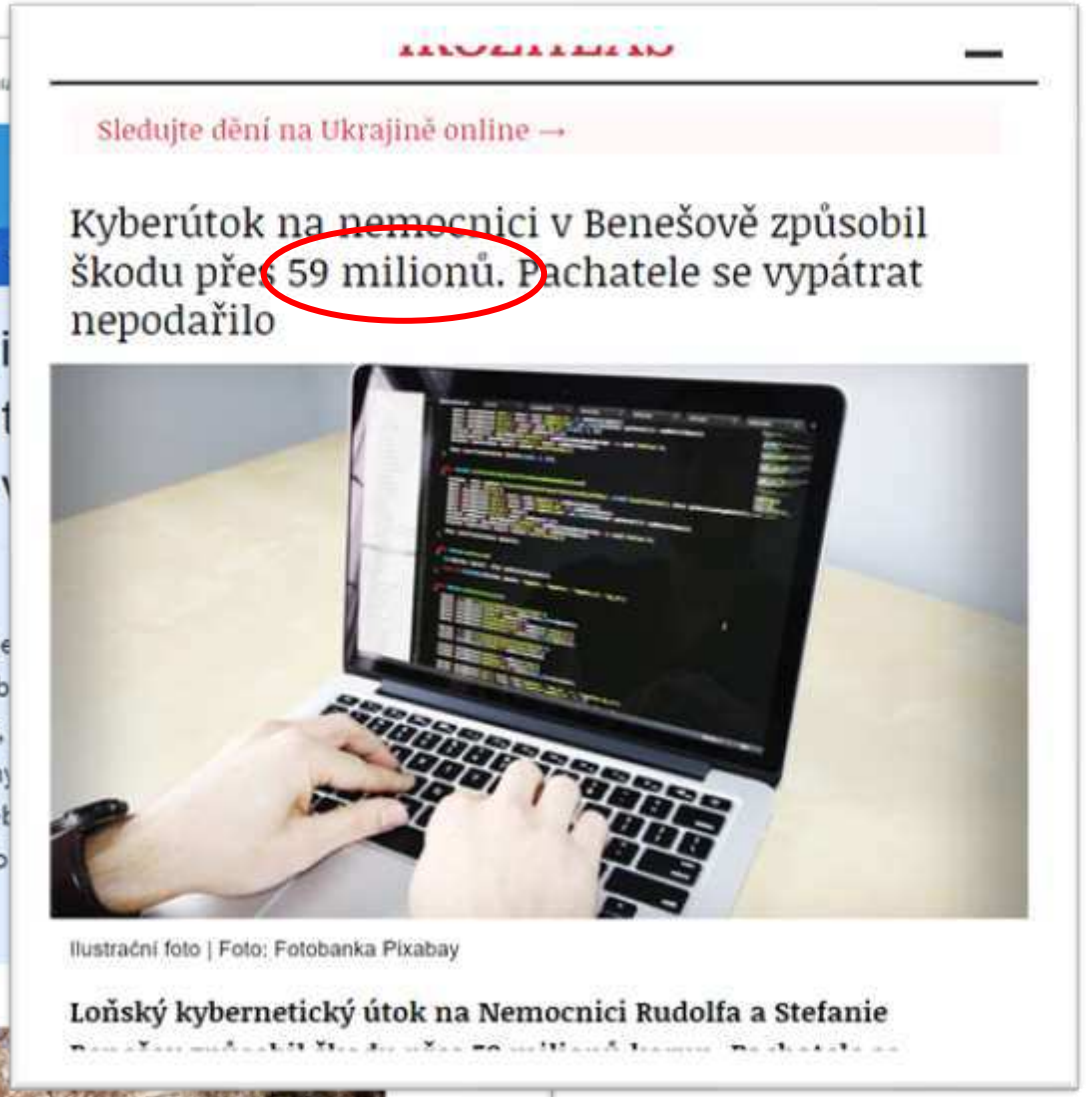
Ransomware v tisku

Zdroj: ZDnet, Apr 2019

Zdroj: Balti



Zdroj: ČT24, Dec 2019



Zdroj: iRozhlas, Aug 2020

RANSOMWARE ÚTOČÍ

Společné atributy

- Napříč segmenty – finance, zdravotnictví, univerzity, průmysl …
- Sofistikované dlouhotrvající přípravy
- Rychlý útok napříč technologiemi – produkce i zálohy
- Slabá úroveň připravenosti pro obnovu – chybí proces obnovy
- Vysoké náklady na obnovu – rychlé řešení, vícenáklady, expertní služby
- Rozsáhlé další škody - dlouhá odstávka, reputace, pokuty …

TRENDY V ZÁKONECH A REGULAČNÍCH AUTORITÁCH

Off-line záloha jako doporučení ochrany

FFIEC: *„**Galvanicky oddělená architektura zálohování** snižuje riziko kyberútoku … a návrat dat do bodu před útokem*

GDPR: *„Zajistit **trvalou důvěrnost, neměnnost, dostupnost** a odolnost zpracovatelských systémů a služeb …. a schopnost obnovit dostupnost a přístup k osobním datům bez zbytečného odkladu v reakci na vzniklý incident „*

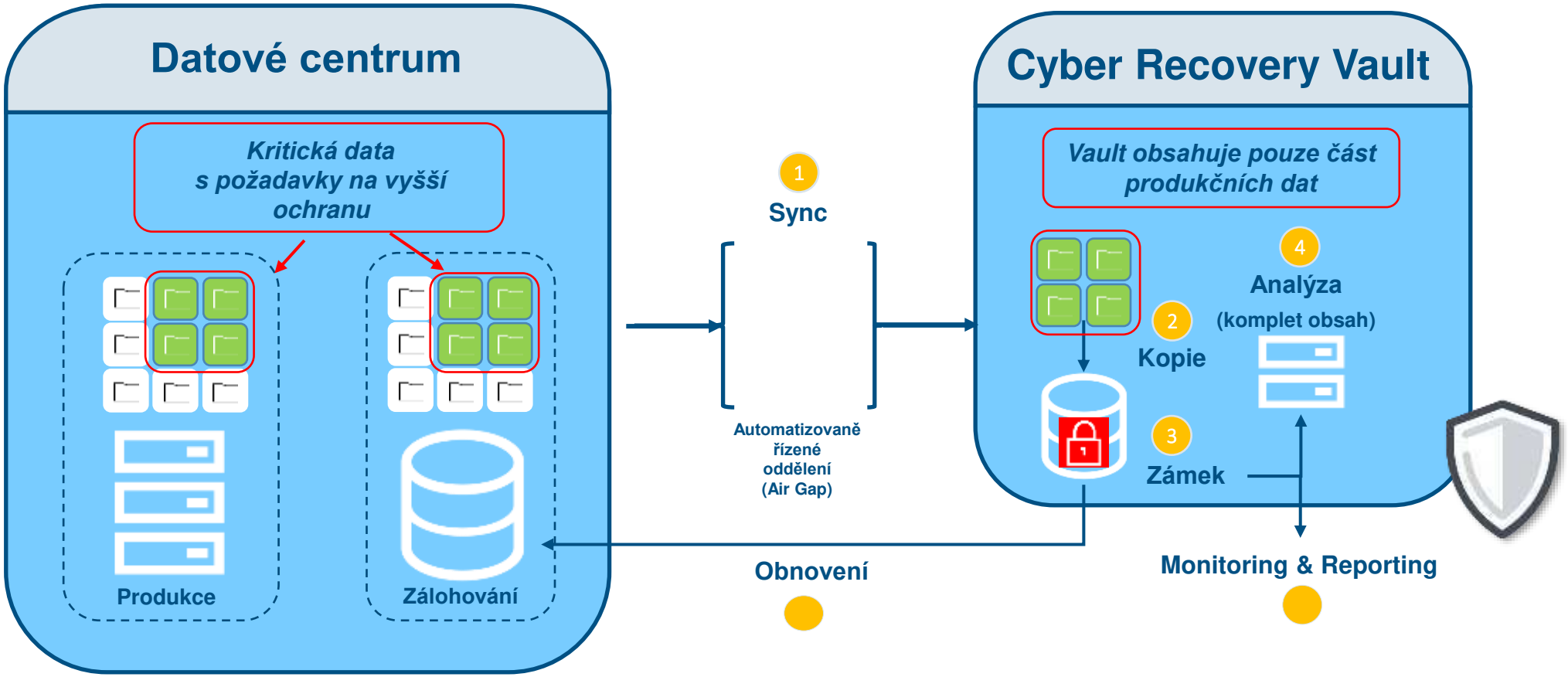
HIPPA: *„Ransomware může odstranit nebo znehodnotit online zálohování …. **zvážit držení off-line záloh**, které jsou nepřístupné útoku…“*

FBI: *“Zajistit **aby zálohy nebyly připojené k sítím**, které chrání. Například jejich fyzickým umístěním off-line.”*

NÚKIB: *„Každá organizace by měla mít propracovaný systém zálohování dat, a to ideálně podle pravidla 3 – 2 – 1, tj. nejméně tři kopie veškerých dat, na dvou různých typech médií **a alespoň jednu kopii dat zcela mimo pracoviště.** “*

UMÍSTĚNÍ ZÁLOH DO OFF-LINE TREZORU

Cyber Recovery Vault v praxi



Ochrana proti výpadku služby,
HW závadě, ztrátě lokality,
chybě uživatele, ….

Off-line záloha pro zajištění
ochrany proti Ransomware
Analýza dat

ANALÝZA POMOCÍ CYBER SENCE

Obnova dat a provozu s jistotou

Prohledávání

CyberSense prochází kritické datové zdroje včetně databází a nestrukturovaných dat a tvoří si tak obrázek běžného provozu. Data mohou být umístěna v sdílených složkách nebo v imagích.

Statistika

Vytváří se 100+ statistik z každého průchodu dat. Statistiky zahrnují analýzu entropie souborů, podobnost, poškození, rozsáhlé mazání/vytvoření atd.

Analýza

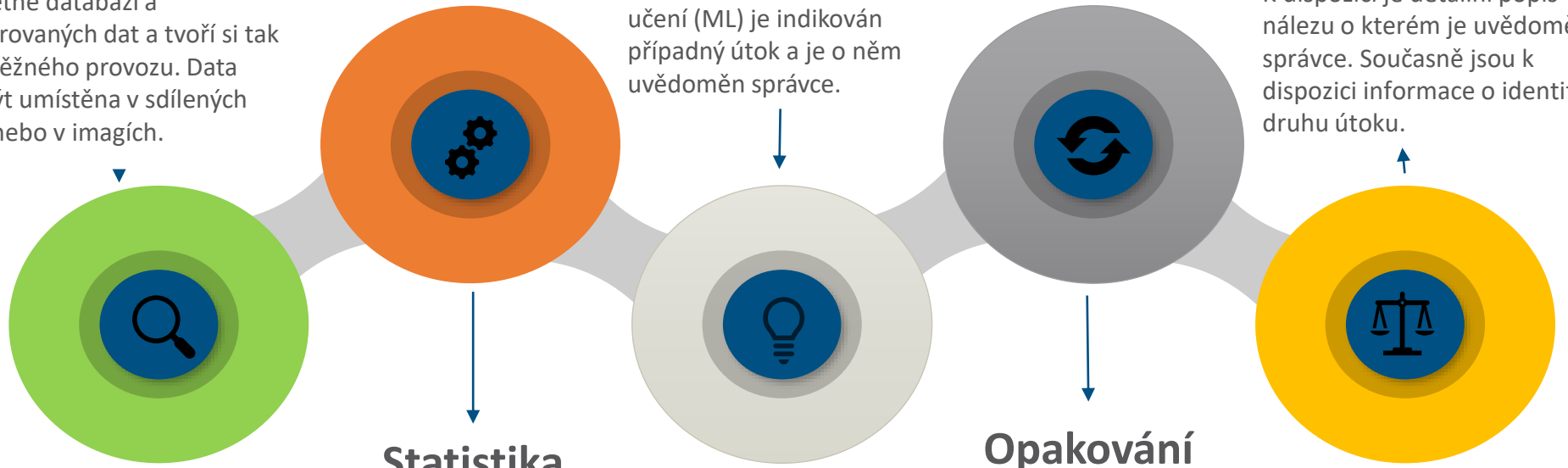
Pomocí algoritmů strojového učení (ML) je indikován případný útok a je o něm uvědoměn správce.

Opakování

Proces se stále dokola opakuje a vyhodnocuje nový stav ve vztahu k předchozím stavům

Vyšetření + náprava

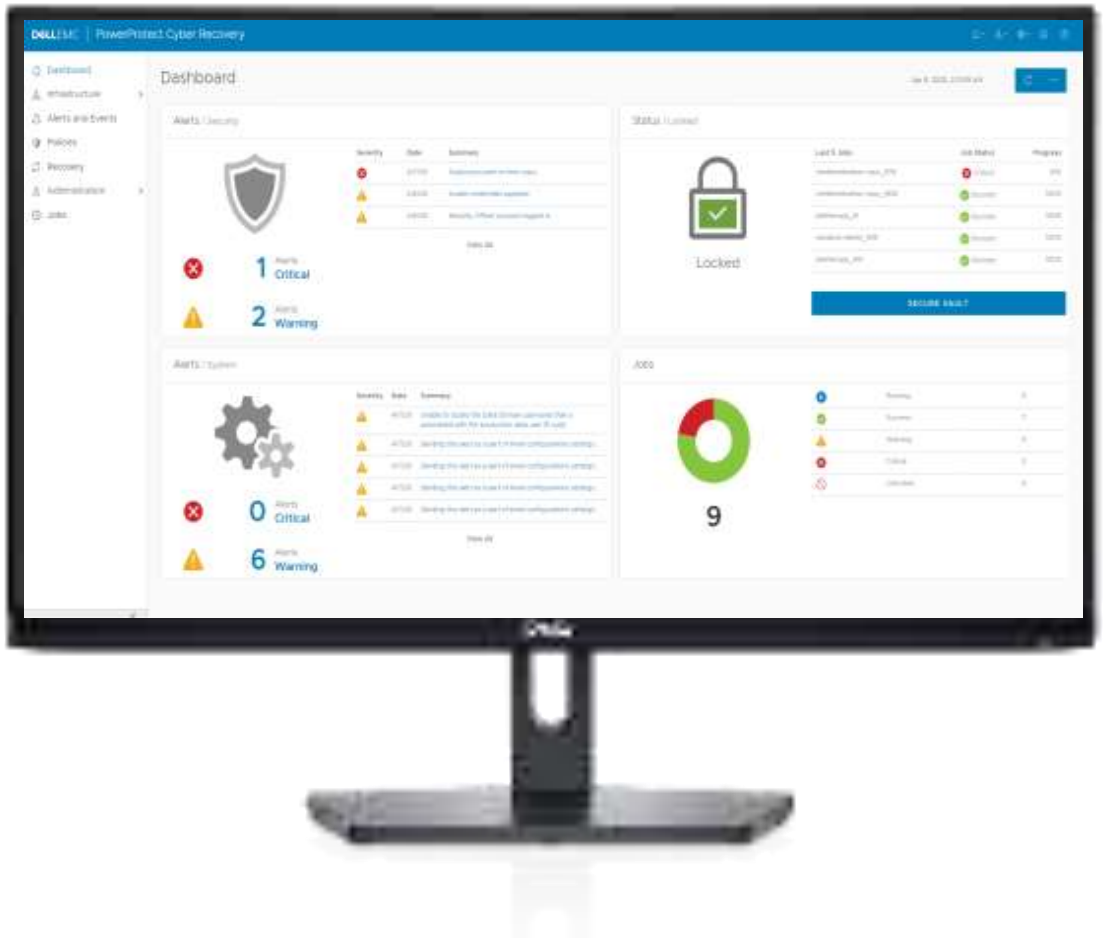
K dispozici je detailní popis nálezu o kterém je uvědoměn správce. Současně jsou k dispozici informace o identifikaci druhu útoku.



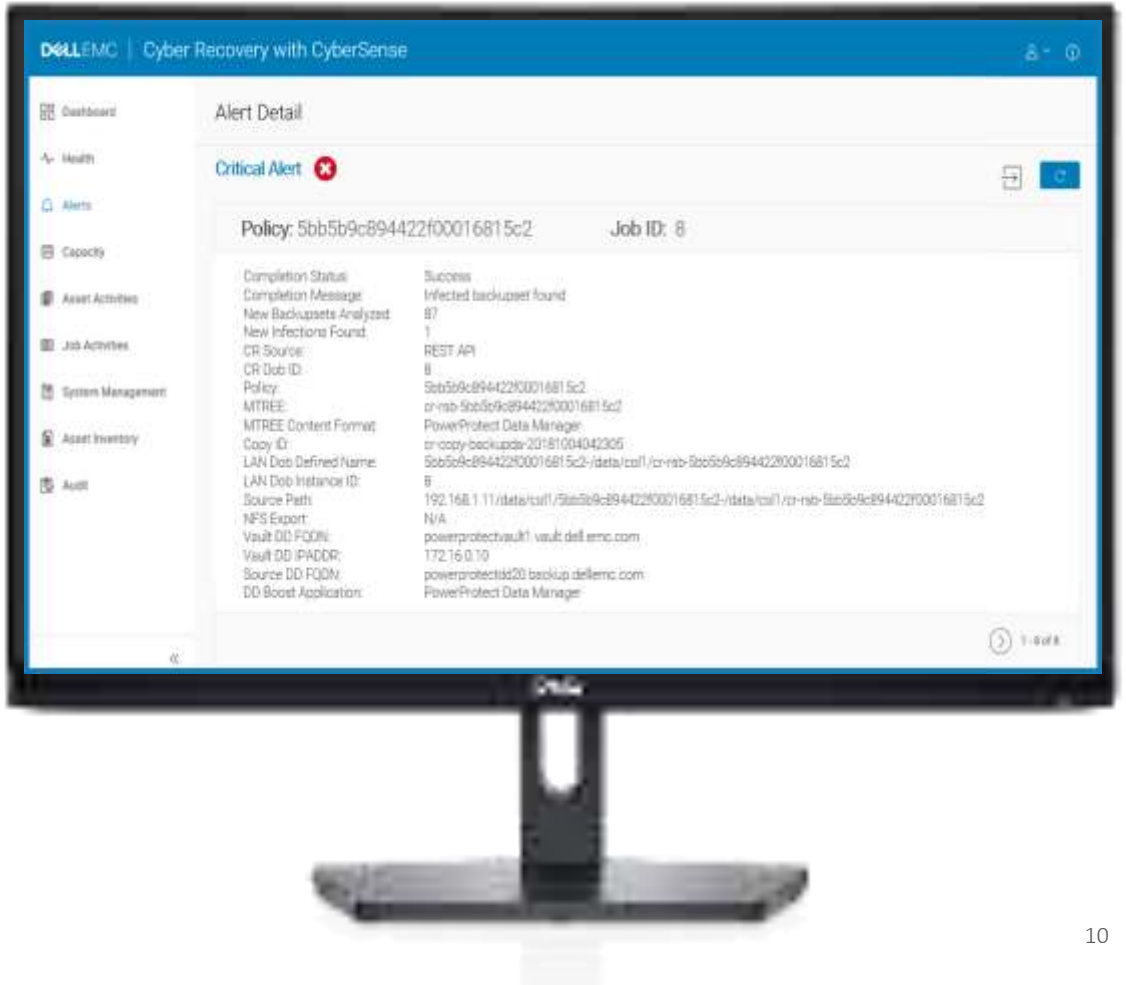
PŘEHLED O PROVOZU CYBER VAULTU

Přehledný dashboard, napojení na monitorovací nástroje

Cyber Recovery Dashboard



CyberSense upozornění



NENÍ TO JEN O PRODUKTU – S&T

Profesionální služby S&T – klíč k úspěchu

- Analýza prostředí a potřeb, určení klíčových zátěží
- Zkušený tým, široké znalosti o provozu IT prostředí
- Profesionální provedení implementace
- Kvalitní dokumentace, příprava BC/DR procesu, ověření
- Pravidelný dohled a správa, vyhodnocení a úpravy, testování

Zveme Vás srdečně k další diskusi na našem stánku č. 15 v 1. patře.