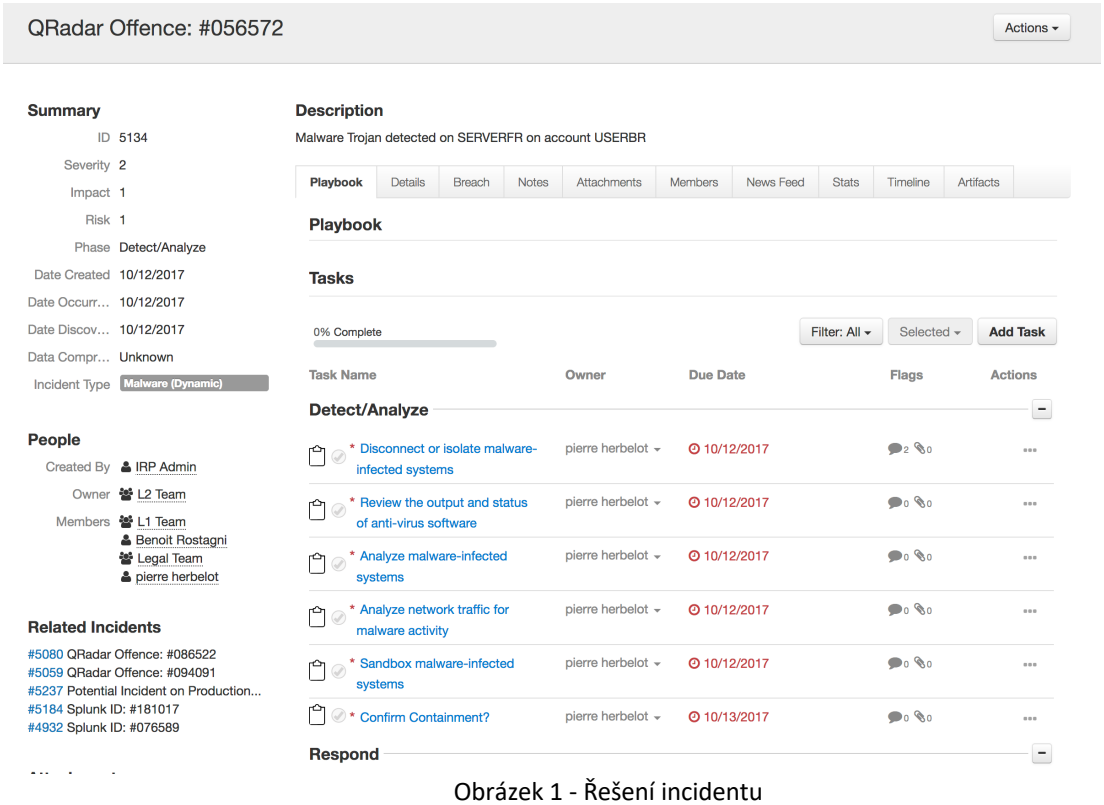
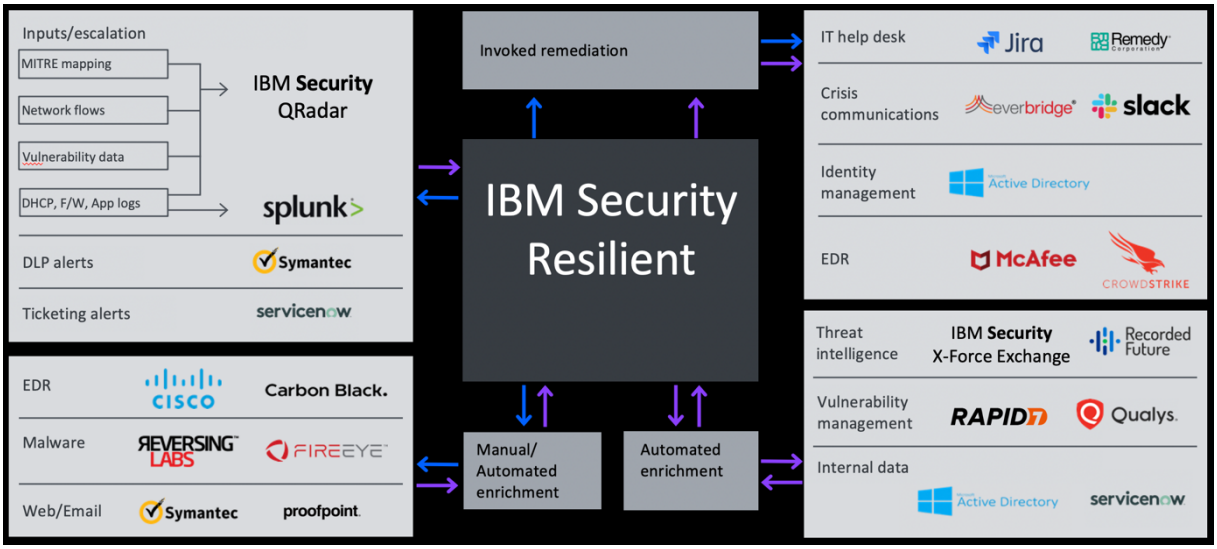
Platforma IBM Qradar SOAR pro zaznamenání a řešení incidentů

Poté, co platforma SIEM zachytí a vyhodnotí bezpečnostní událost, měla by následovat reakce – řešení incidentu. IBM Qradar Security Orchestration and Automation Response (SOAR) umožňuje orchestraci a automatizaci této reakce, čímž ji umožňuje urychlit a zefektivnit. Incident však nemusí vzniknout jen ze SIEM systému. Může vzniknout i manuálním zadáním či například automaticky pomocí příchozího mailu nebo z ticketing systémů. SOAR platforma zabezpečuje, že každý bezpečnostní incident je řešen konzistentně, bez ohledu na to, který bezpečnostní analytik jej zrovna začne řešit, protože dle typu incidentu (např. Malware, ztráta notebooku nebo DDoS útok) a dalších parametrů vytvoří seznam požadovaných aktivit (např. spustit scan počítače, změnit pravidlo na firewallu atd.). Tyto aktivity mohou jít napříč dalšími týmy společnosti, jako jsou například IT, ale i právní oddělení, oddělení externí komunikace a podobně, či mohou být plně automatizována a provedena externími systémy (např. změna pravidel na firewallu atd.). Tato pravidla jsou pak dynamicky aplikována v průběhu života incidentu i při změně jeho parametrů – aktivity mohou být automaticky přidávány a ubírány.

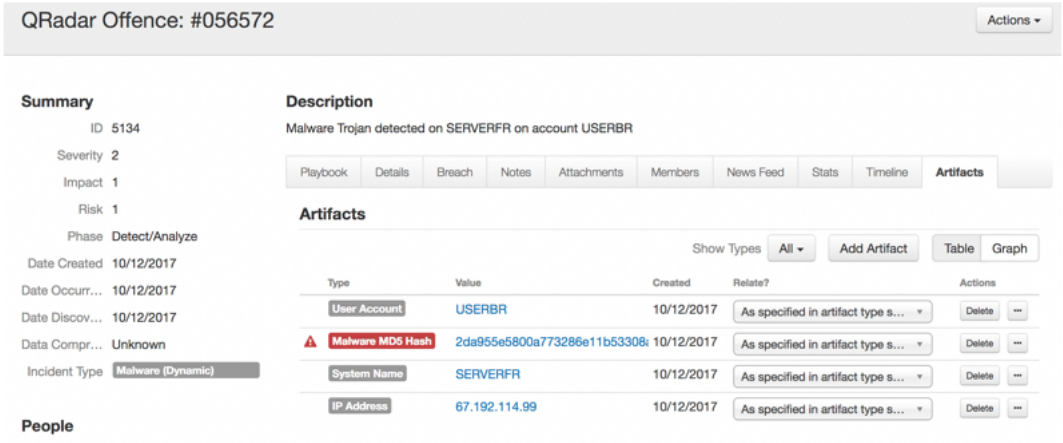


Obrázek 1 - Řešení incidentu

Mimo SIEM je IBM Qradar SOAR platforma připravena i na integrace s mnoha dalšími bezpečnostními systémy organizace, jako jsou například správa a ochrana koncových bodů, správa uživatelů atd. Všechny tyto systémy pak mohou obohacovat incident o další důležité informace vedoucí k urychlení a usnadnění řešení incidentu. Dalšími vstupy pak jsou například tzv. Intelligence feedy, které vyhodnotí kontrolní součty souborů, IP adresy atd.

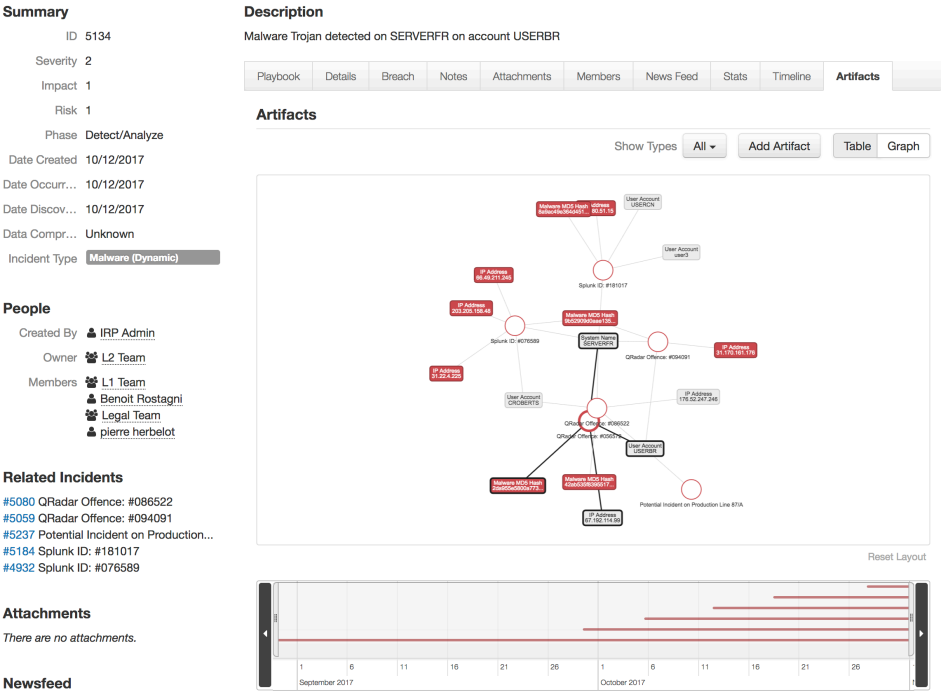


Obrázek 2 – Příklad integrace systémů na SOAR



Obrázek 3 - Artefakty

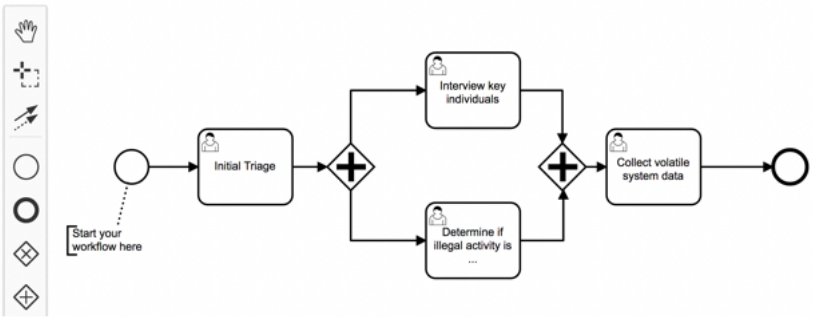
IBM Qradar SOAR podporuje vyšetřování incidentů i poskytováním přehledné informace o vztazích mezi jednotlivými incidenty podle artefaktů, a to v grafické i textové podobě, včetně jejich vývoje v čase:



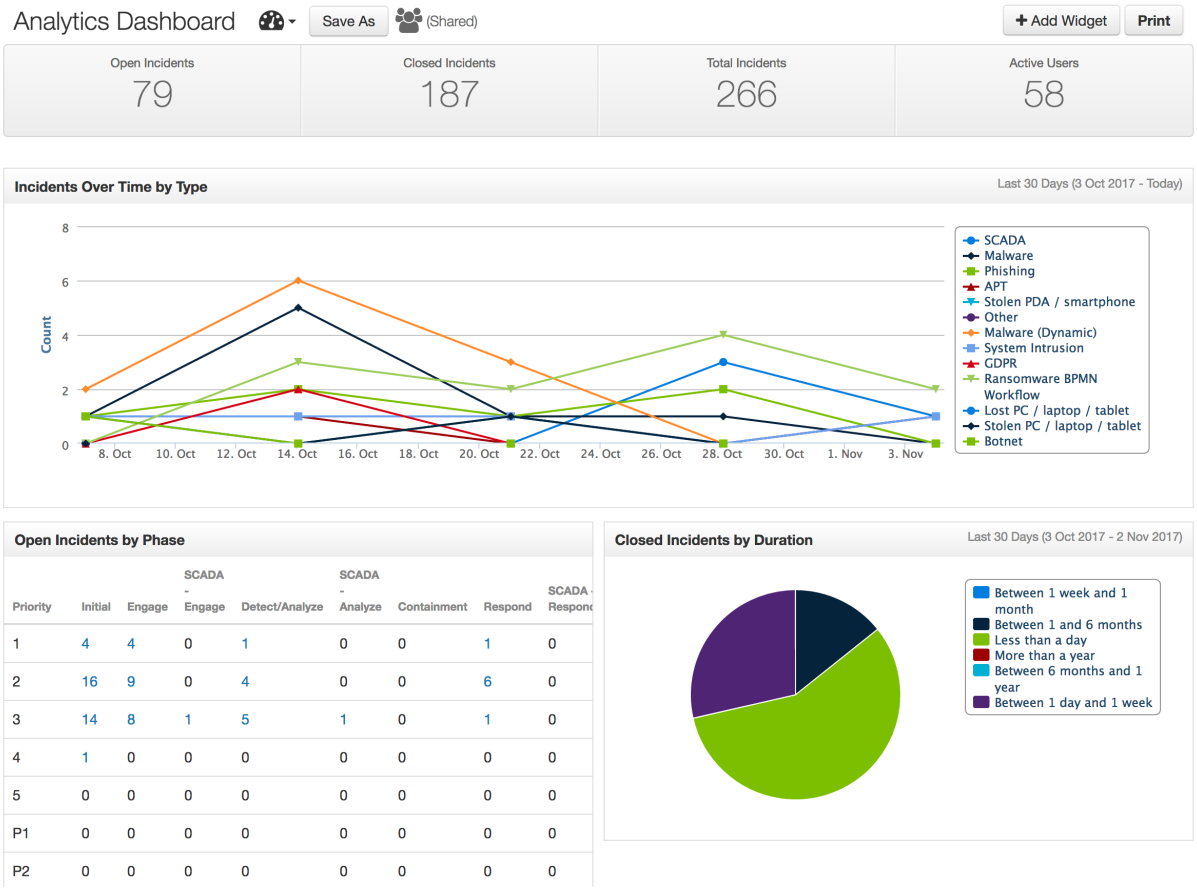
Obrázek 4 - Propojení artefaktů

Platforma rovněž podporuje vzájemnou komunikaci všech řešitelů incidentů při zachování pravidel viditelnosti – jednotliví uživatelé či celé skupiny vidí jen ty incidenty, které jsou pro ně relevantní. Systém pak zasílá upozornění uživatelům nejen při přiřazení aktivity nebo celého incidentu, ale i při zmínce o daném uživateli v poznámce nebo při změně incidentu, což výrazně urychluje a zjednodušuje vzájemnou komunikaci.

Pomocí workflow a integrací na další systémy pak systém provádí orchestraci a automatické vyřešení incidentů, například umístění koncového bodu do karantény či změnou pravidel na síťovém prvku.



IBM Qradar SOAR poskytuje analytické pohledy pro rychlý přehled o aktuálním stavu prostředí:



Simulace incidentů umožňuje trénink nejen členů bezpečnostního týmu, ale i dalších účastníků, jako jsou zaměstnanci právního oddělení, HR či další.