

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.

QRadat Offence: #056572 Actions ▾

Summary

ID 5134
Severity 2
Impact 1
Risk 1
Phase Detect/Analyze
Date Created 10/12/2017
Date Occurr... 10/12/2017
Date Discov... 10/12/2017
Data Compr... Unknown
Incident Type **Malware (Dynamic)**

People

Created By **IRP_Admin**
Owner **L2 Team**
Members **L1 Team**
Benoit Rostagni
Legal Team
pierre herbelot

Related Incidents

- #5080 QRadar Offence: #086522
- #5059 QRadar Offence: #094091
- #5237 Potential Incident on Production...
- #5184 Splunk ID: #181017
- #4932 Splunk ID: #076589

Description

Malware Trojan detected on SERVERFR on account USERBR

Playbook

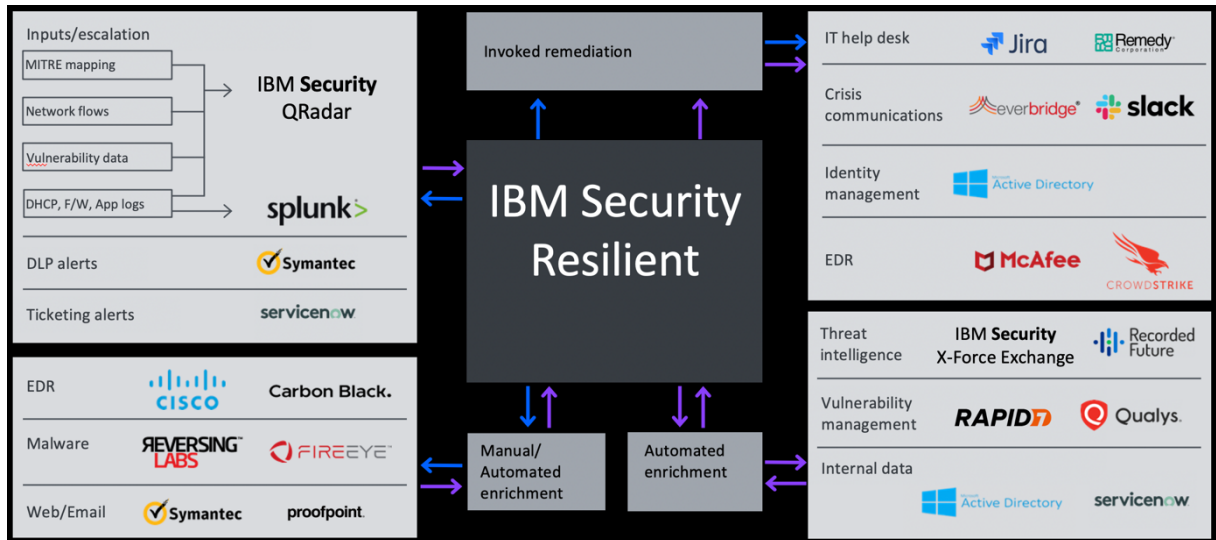
Tasks

0% Complete Filter: All ▾ Selected ▾ Add Task

Task Name	Owner	Due Date	Flags	Actions
Detect/Analyze				
* Disconnect or isolate malware-infected systems	pierre herbelot ▾	10/12/2017	2 0	...
* Review the output and status of anti-virus software	pierre herbelot ▾	10/12/2017	0 0	...
* Analyze malware-infected systems	pierre herbelot ▾	10/12/2017	0 0	...
* Analyze network traffic for malware activity	pierre herbelot ▾	10/12/2017	0 0	...
* Sandbox malware-infected systems	pierre herbelot ▾	10/12/2017	0 0	...
* Confirm Containment?	pierre herbelot ▾	10/13/2017	0 0	...
Respond				

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

QRadar Offence: #056572 Actions ▾

Summary

ID 5134

Severity 2

Impact 1

Risk 1

Phase Detect/Analyze

Date Created 10/12/2017

Date Occur... 10/12/2017

Date Discov... 10/12/2017

Data Compr... Unknown

Incident Type **Malware (Dynamic)**

People

Description

Malware Trojan detected on SERVERFR on account USERBR

Playbook Details Breach Notes Attachments Members News Feed Stats Timeline **Artifacts**

Artifacts

Show Types All ▾ Add Artifact Table Graph

Type	Value	Created	Relate?	Actions
User Account	USERBR	10/12/2017	As specified in artifact type s...	Delete ...
Malware MDS Hash	2da955e5800a773286e11b53308	10/12/2017	As specified in artifact type s...	Delete ...
System Name	SERVERFR	10/12/2017	As specified in artifact type s...	Delete ...
IP Address	67.192.114.99	10/12/2017	As specified in artifact type s...	Delete ...

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:

Summary

ID 5134

Severity 2

Impact 1

Risk 1

Phase Detect/Analyze

Date Created 10/12/2017

Date Occur... 10/12/2017

Date Discov... 10/12/2017

Data Compr... Unknown

Incident Type **Malware (Dynamic)**

People

Created By IRP Admin

Owner L2 Team

Members L1 Team, Benoit Rostagni, Legal Team, pierre herbelot

Related Incidents

#5080 QRadar Offence: #086522

#5059 QRadar Offence: #094091

#5237 Potential Incident on Production...

#5184 Splunk ID: #181017

#4932 Splunk ID: #076589

Attachments

There are no attachments.

Newsfeed

Description

Malware Trojan detected on SERVERFR on account USERBR

Playbook Details Breach Notes Attachments Members News Feed Stats Timeline **Artifacts**

Artifacts

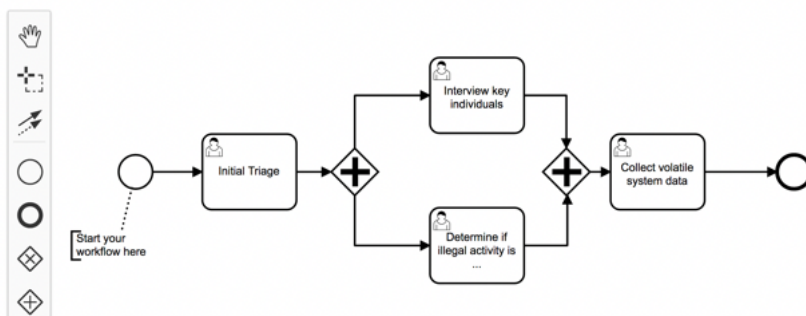
Show Types All Add Artifact Table Graph

Reset Layout

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.

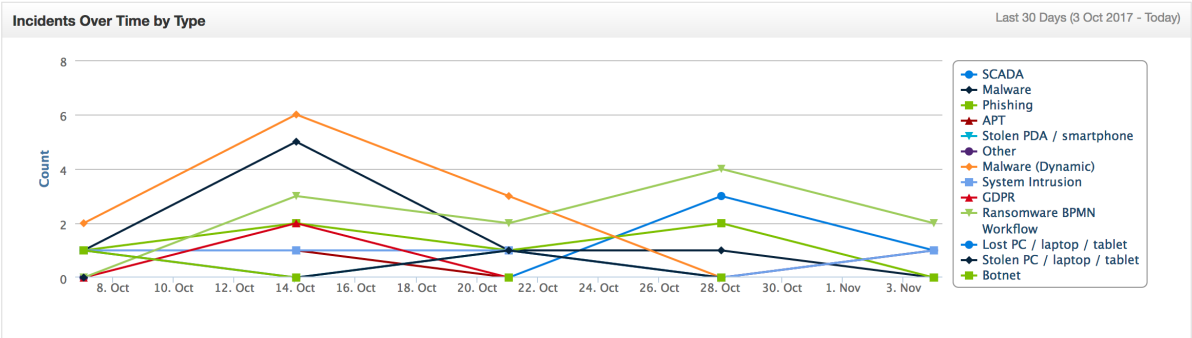
Pomocí workflow a integrací na další systémy pak systém provádí orchestraci a automatické vyřešení incidentů, například umístění koncového bodu do karantény či změnou pravidel na síťovém prvku.



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

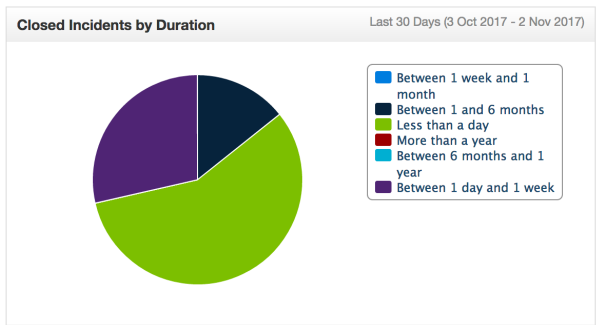
Analytics Dashboard Save As (Shared) + Add Widget Print

Open Incidents 79	Closed Incidents 187	Total Incidents 266	Active Users 58
-----------------------------	--------------------------------	-------------------------------	---------------------------



Open Incidents by Phase

Priority	Initial	Engage	SCADA - Engage	Detect/Analyze	SCADA - Analyze	Containment	Respond	SCADA - Response
1	4	4	0	1	0	0	1	0
2	16	9	0	4	0	0	6	0
3	14	8	1	5	1	0	1	0
4	1	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
P1	0	0	0	0	0	0	0	0
P2	0	0	0	0	0	0	0	0



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