Přístup ke sběru dat za účelem tvorby monitorovacích scénářů.

Michal Gürtner

Software Architect

michal_gurtner@cz.ibm.com

IBM **Security**

IBM

Agenda

Podpora MITRE ATT&CK

IBM QRadar (SIEM)

Podpora Diamond, Kill chain modelů

IBM i2, Resilient SOAR platform

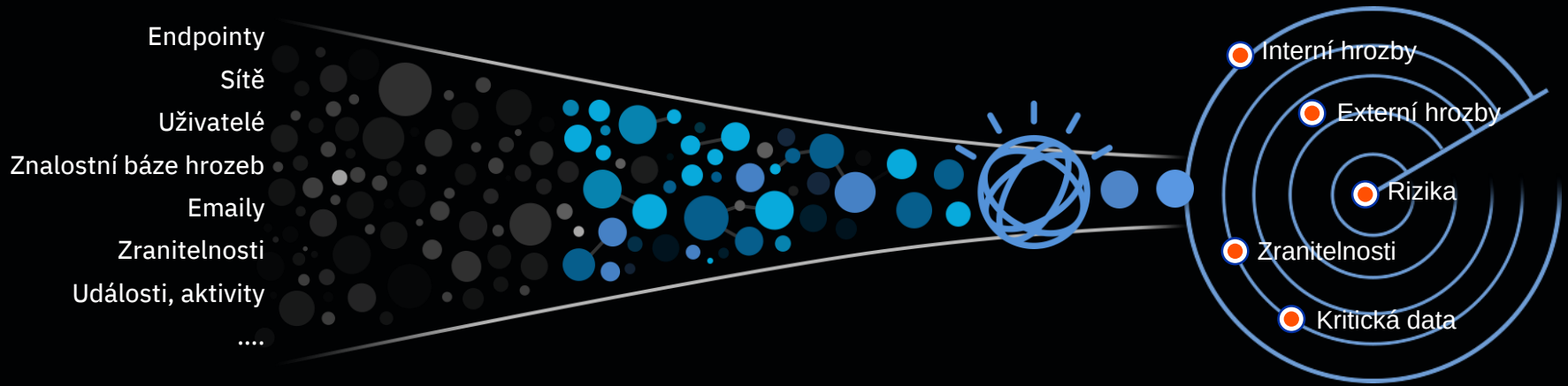
4 pilíře boje s kybernetickými hrozbami

Sběr dat

Detekce

Šetření

Reakce



MITRE ATT&CK framework

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearphishing Link	Dynamic Data Exchange	Authentication Package	DLL Search Order Hijacking	Code Signing	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Spearphishing via Service	Execution through API	BITS Jobs	Dylib Hijacking	Compile After Delivery	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Firmware Corruption
Supply Chain Compromise	Execution through Module Load	Bootkit	Elevated Execution with Prompt	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Inhibit System Recovery
Trusted Relationship	Exploitation for Client Execution	Browser Extensions	Emond	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture	Fallback Channels		Network Denial of Service
Valid Accounts	Graphical User Interface	Change Default File Association	Exploitation for Privilege Escalation	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser	Multi-hop Proxy		Resource Hijacking
	InstallUtil	Component Firmware	Extra Window Memory Injection	Connection Proxy	Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture	Multi-Stage Channels		Runtime Data Manipulation

MITRE ATT&CK framework

Remote Desktop Protocol

Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS). [1] There are other implem

ID: T1076

Tactic: Lateral Movement

Platform: Windows

System Requirements: RDP service enabled, account in th Desktop Users group

Permissions Requi

Data Sources: Auth monitoring

CAPEC ID: CAPEC-5

Contributors: Matth

Version: 1.0

Procedure Examples

Name	Description
APT1	The APT1 group is known t
APT3	APT3 enables the Remote D
APT39	APT39 has been seen using
APT41	APT41 used RDP for lateral
Axiom	The Axiom group is known
Carbanak	Carbanak enables concurre
Cobalt Group	Cobalt Group has used Rem
Cobalt Strike	Cobalt Strike can start a VN

Mitigations

Mitigation	
Audit	
Disable or Remove Feature or Program	
Limit Access to Resource Over Network	
Multi-factor Authentication	Use multi-factor authentication for remote logins.[7]
Network Segmentation	Do not leave RDP accessible from the internet. Enable firewall rules to block R
Operating System Configuration	Change GPOs to define shorter timeouts sessions and maximum amount of ti stays active on the RD session host server.[6]
Privileged Account Management	Consider removing the local Administrators group from the list of groups allov
User Account Management	Limit remote user permissions if remote access is necessary.

Detection

Use of RDP may be legitimate is used. Other factors, such as remote login, may indicate su for user accounts logged into access patterns to multiple sy

Also, set up process monitori creation that uses `cmd.exe /` session hijacking.

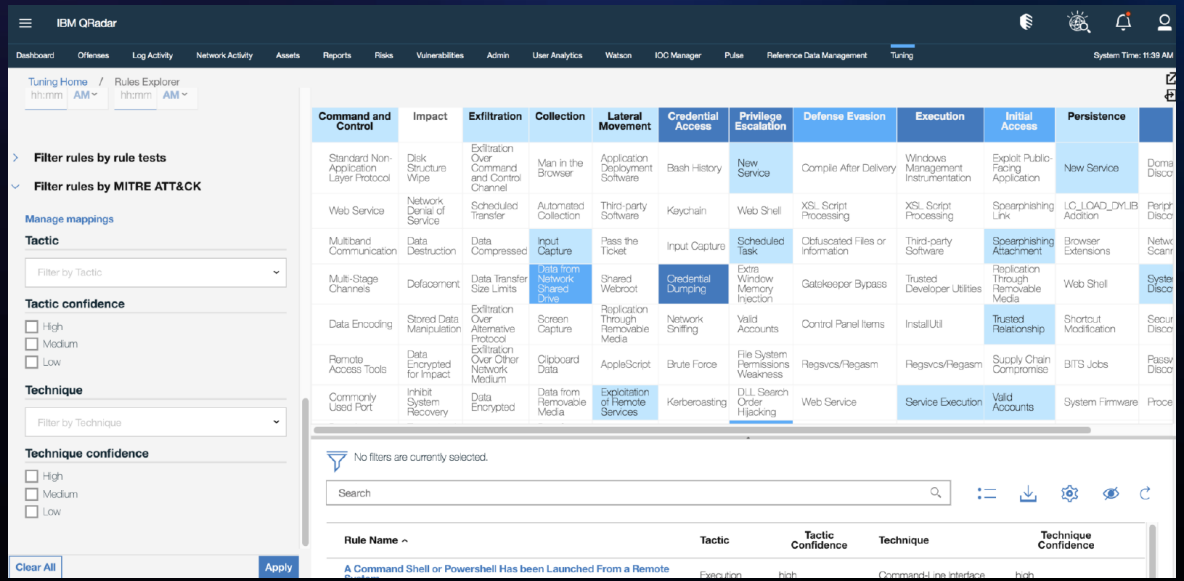
References

1. Microsoft. (n.d.). Remote Desktop Services. Retrieved June 1, 2016.
2. Alperovitch, D. (2014, October 31). Malware-Free Intrusions. Retrieved November 4, 2014.
3. Korznikov, A. (2017, March 17). Passwordless RDP Session Hijacking Feature All Windows versions. Retrieved December 11, 2017.
4. Beaumont, K. (2017, March 19). RDP hijacking—how to hijack RDS and RemoteApp sessions transparently to move through
23. valsmith. (2012, September 21). More on APTSim. Retrieved September 28, 2017.
24. FireEye Labs. (2014, May 20). The PLA and the 8:00am-5:00pm Work Day: FireEye Confirms DOJ's Findings on APT1 Intrusion Activity. Retrieved November 4, 2014.
25. FireEye Threat Intelligence. (2016, April). Follow the Money: Dissecting the Operations of the Cyber Crime Group FIN6. Retrieved June 1, 2016.

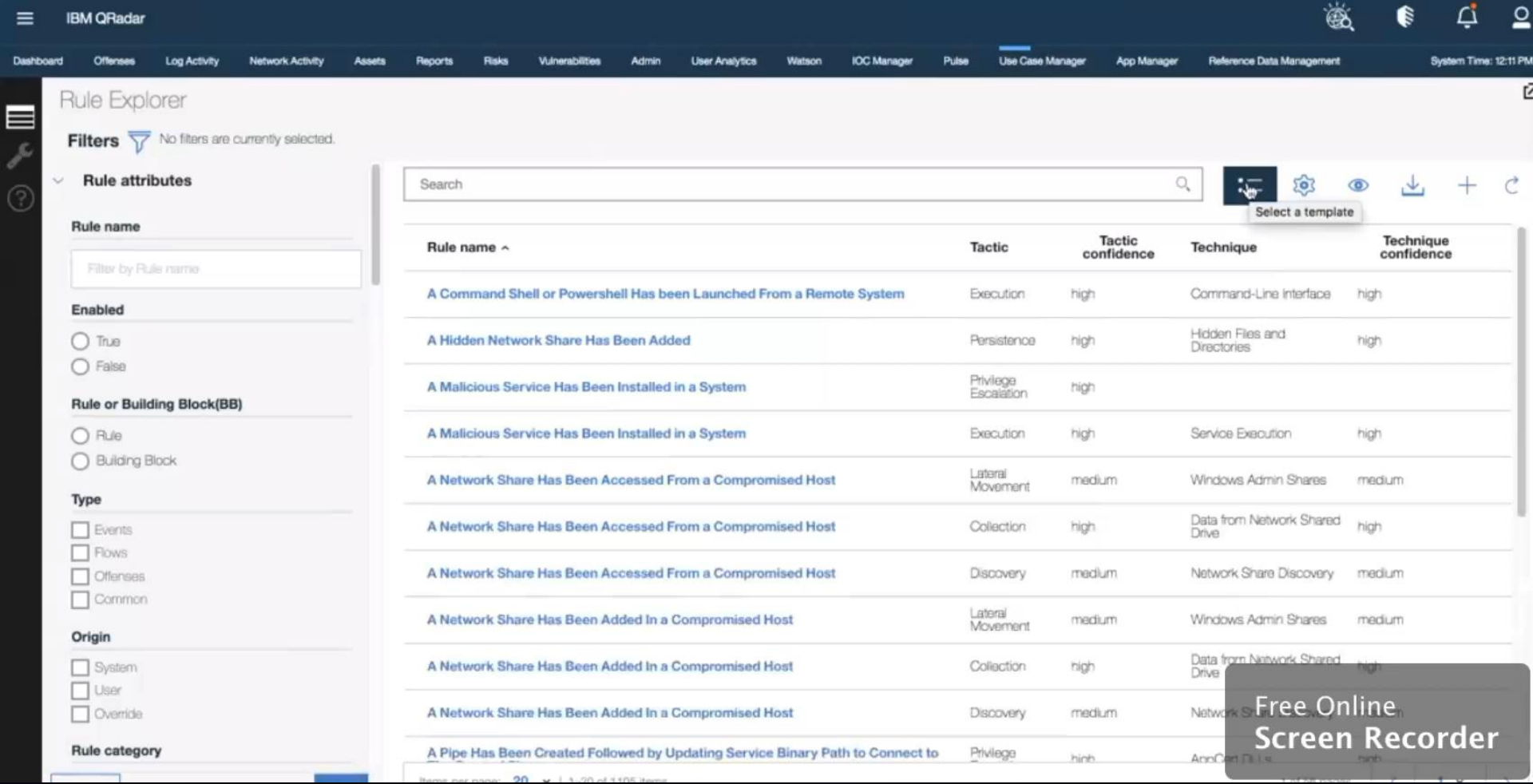
Agenda

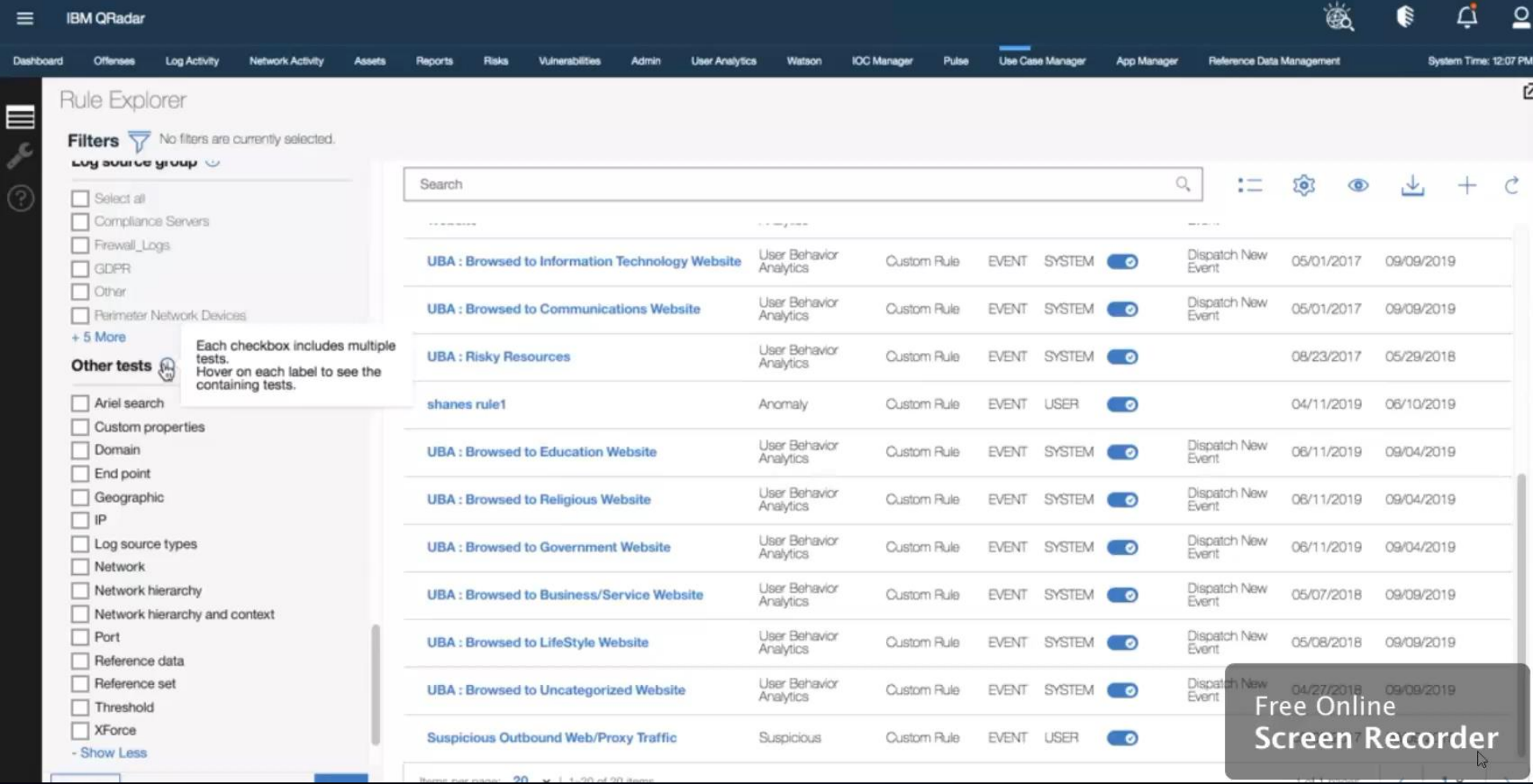
Podpora MITRE ATT&CK

IBM QRadar (SIEM) demo ukázka



IBM **Security**


IBM QRadar
Dashboard
Offenses
Log Activity
Network Activity
Assets
Reports
Risks
Vulnerabilities
Admin
User Analytics
Watson
IOC Manager
Pulse
Use Case Manager
App Manager
Reference Data Management
System Time: 12:11 PM
Rule Explorer
Filters
No filters are currently selected.
Rule attributes
Rule name
Filter by Rule name
Enabled
True
False
Rule or Building Block(BB)
Rule
Building Block
Type
Events
Flows
Offenses
Common
Origin
System
User
Override
Rule category
Search
Select a template
Rule name
Tactic
Tactic confidence
Technique
Technique confidence
A Command Shell or Powershell Has been Launched From a Remote System
Execution
high
Command-Line Interface
high
A Hidden Network Share Has Been Added
Persistence
high
Hidden Files and Directories
high
A Malicious Service Has Been Installed in a System
Privilege Escalation
high
A Malicious Service Has Been Installed in a System
Execution
high
Service Execution
high
A Network Share Has Been Accessed From a Compromised Host
Lateral Movement
medium
Windows Admin Shares
medium
A Network Share Has Been Accessed From a Compromised Host
Collection
high
Data from Network Shared Drive
high
A Network Share Has Been Accessed From a Compromised Host
Discovery
medium
Network Share Discovery
medium
A Network Share Has Been Added In a Compromised Host
Lateral Movement
medium
Windows Admin Shares
medium
A Network Share Has Been Added In a Compromised Host
Collection
high
A Network Share Has Been Added In a Compromised Host
Discovery
medium
A Pipe Has Been Created Followed by Updating Service Binary Path to Connect to
Privilege
Free Online
Screen Recorder
IBM Security
IBM



IBM **Security**

IBM QRadar

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Risks | Vulnerabilities | Admin | User Analytics | Watson | IOC Manager | Pulse | Use Case Manager | App Manager | Reference Data Management

System Time: 12:16 PM

Tuning

Last updated: 11/22/2019, 16:34:37

Open offenses: 21

Active offenses: 14

Offense creation trend

Tune your QRadar offenses by analyzing rules that cause the biggest number of offenses

Tune most active rules

QRadar Use Case Manager can help you determine which rules generate the most offenses, and then guide you through the steps to tune them.

Tune based on the CRE event report

The Custom Rules Engine (CRE) event report shows which CRE events were generated most often. It also provides information about the rule activity. You can tune these rules or use the event information from the report to update your QRadar environment.

Tune your QRadar offenses by going through the most common configuration steps

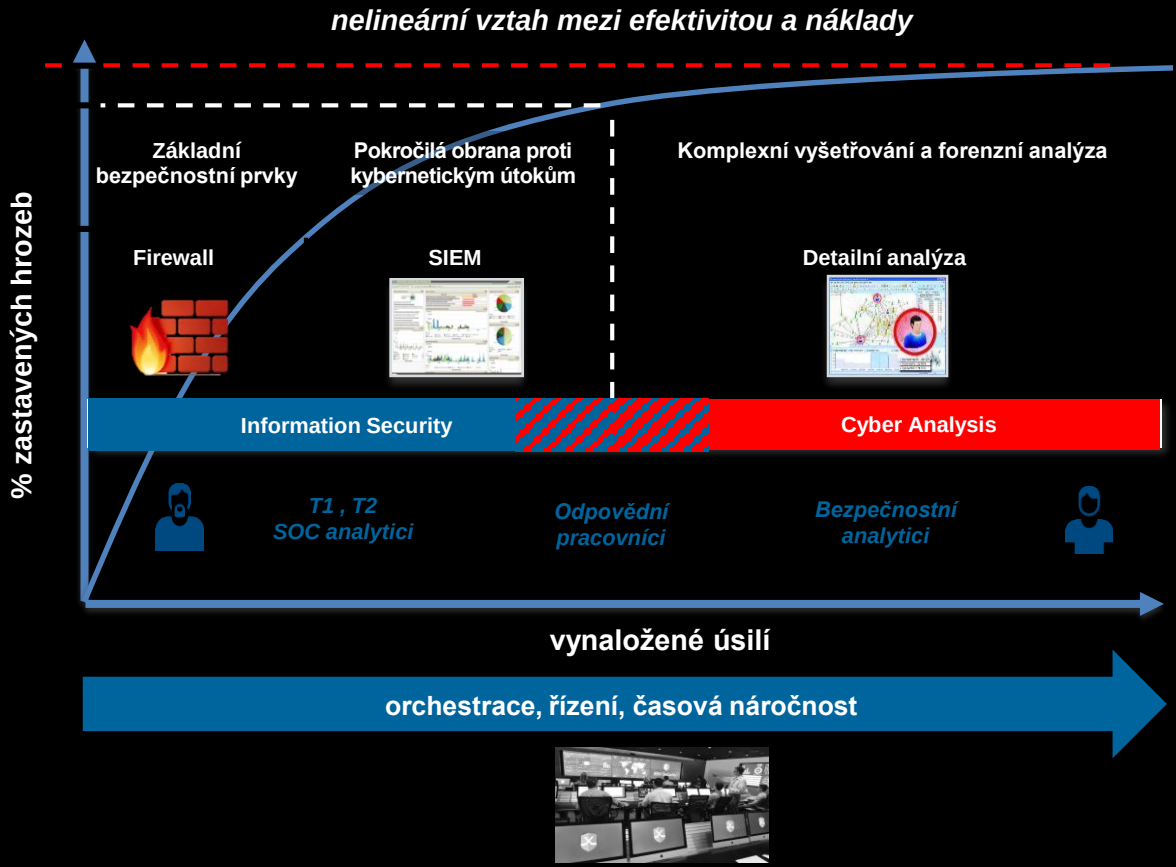
Review network hierarchy

Network Hierarchy is used to define which IP addresses and subnets are part of your network. Defining your network hierarchy and keeping it up-to-date is an important step in helping prevent false offenses.

Review building blocks

Rules use information about your servers to determine whether to generate the rule responses. Review and update common rule building blocks to enable QRadar to discover and classify more servers on your network, and prevent false positives.

Boj s kybernetickými hrozbami



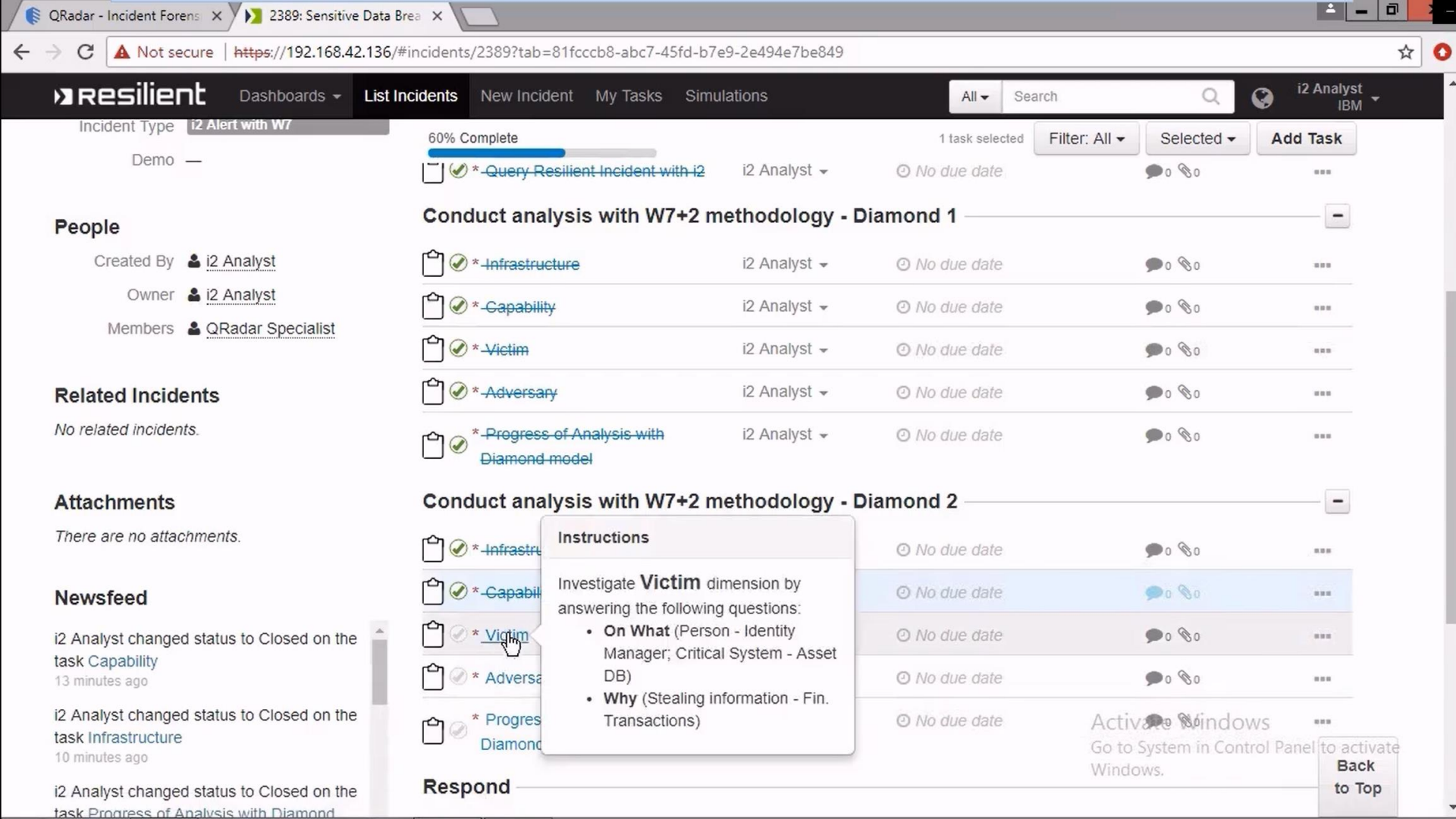
Agenda

Uplatnění Diamond, Kill chain modelů

demo IBM i2, Resilient SOAR platform

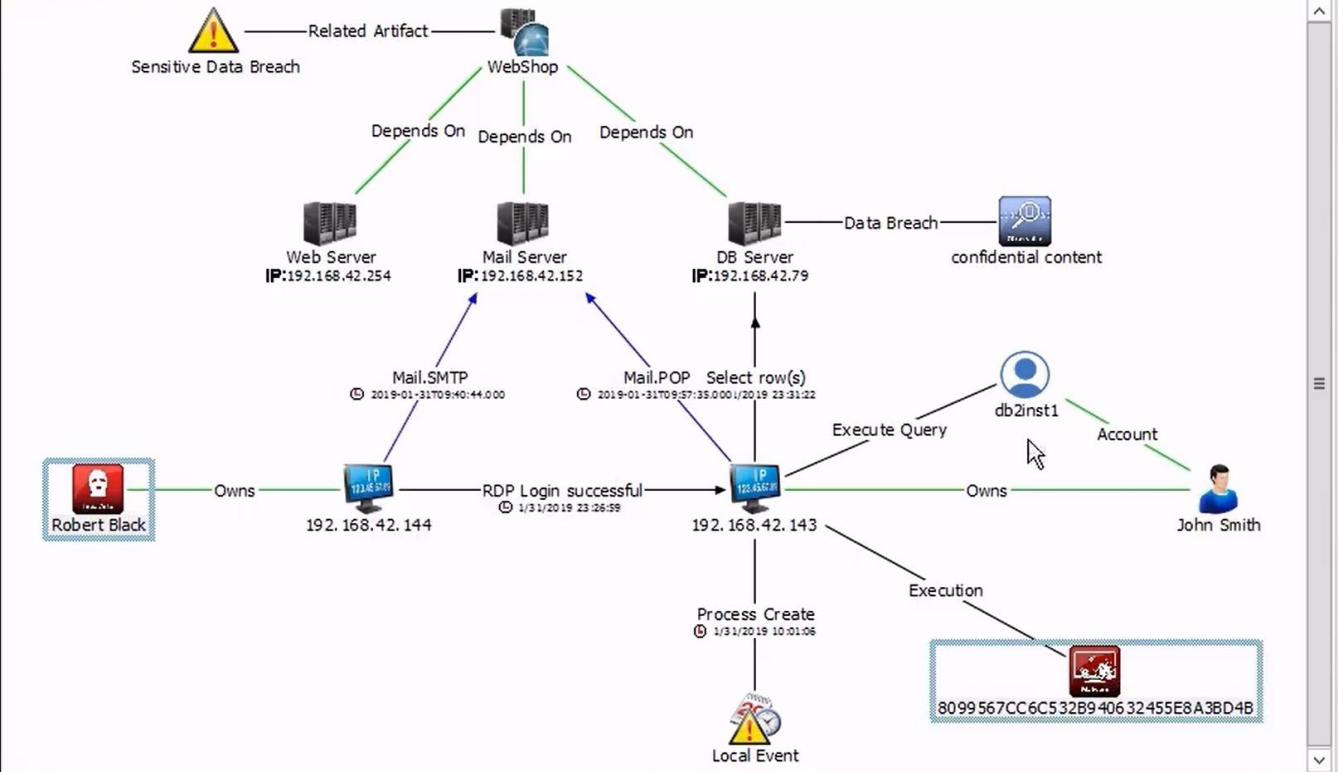
QRadar detekuje incident

- Analytik incident vidí ve svém TODO v Resilientu
- Následuje předepsané kroky
- Vyšetřuje pomocí i2 a získává data z mnoha zdrojů
- Interpretuje a předává výsledek investigace


QRadar - Incident Forens
2389: Sensitive Data Brea
Not secure
https://192.168.42.136/#incidents/2389?tab=81fcccb8-abc7-45fd-b7e9-2e494e7be849
resilient
Dashboards
List Incidents
New Incident
My Tasks
Simulations
All
Search
i2 Analyst
IBM
Incident Type
i2 Alert with W7
Demo
60% Complete
1 task selected
Filter: All
Selected
Add Task
* Query Resilient Incident with i2
i2 Analyst
No due date
People
Created By
i2 Analyst
Owner
i2 Analyst
Members
QRadar Specialist
Conduct analysis with W7+2 methodology - Diamond 1
* Infrastructure
* Capability
* Victim
* Adversary
* Progress of Analysis with Diamond model
Related Incidents
No related incidents.
Conduct analysis with W7+2 methodology - Diamond 2
Attachments
There are no attachments.
Instructions
Investigate Victim dimension by answering the following questions:
On What (Person - Identity Manager; Critical System - Asset DB)
Why (Stealing information - Fin. Transactions)
Newsfeed
i2 Analyst changed status to Closed on the task Capability
13 minutes ago
i2 Analyst changed status to Closed on the task Infrastructure
10 minutes ago
Respond
Activate Windows
Go to System in Control Panel to activate Windows.
Back to Top

Spelling Legend — Prepare
Save a Redacted Copy | Purge Data Records | Purge All Data Records — Redact and Purge
Take Snapshots | Previous Snapshot | Next Snapshot — Snapshots
Reports
Current View | Entire Chart — Save as Picture
Page Setup | Fit to One Page | Best Fit | Print Layout | Print | Print to PDF — Print
Send by Email
Extensions

Chart1



i2Connect

Incidents
Resilient

Get Incident Details
Resilient

Query Incidents
Resilient

Submit Artifact(s)
Resilient

Incident Id? *
2389

Accounts of a Person
ISIM Connector

Insert from Palette
Bar Charts and Histograms

Otázky a komentáře

Zdroje informací na webu:

ibm.com/security

https://www.securitylearningacademy.com/

https://www.youtube.com/ibmsecurity

—

Michal Gürtner, IBM Software architect
michal_gurtner@cz.ibm.com