

# Integrované nástroje v modernom centre bezpečnostných operácií



**Ondřej Burián**

Security Intelligence & Response Client Technical Professional  
Central and Eastern Europe  
IBM Security

# Let's focus on the most critical security use cases

Outcome-driven security

## Prove Compliance



Get Ahead of Compliance



Enhance Security Hygiene



Govern Users and Identities

## Stop Threats



Detect & Stop Advanced Threats



Orchestrate Incident Response



Master Threat Hunting

## Grow Business



Secure Hybrid Cloud



Protect Critical Assets



Prevent Advanced Fraud

# Disconnected security capabilities are failing us

Security analytics

Privileged user management

Access management

User behavior analytics

Data access control

Incident response

Data protection

Endpoint patching and management

Fraud protection

Identity governance and administration

Network visibility and segmentation

Mainframe security

Network forensics and threat management

Application scanning

Malware protection

Vulnerability management

IDaaS

IoCs

Threat sharing

Device management

Endpoint detection and response

Transaction protection

Criminal detection

Content security

Firewalls and intrusion prevention

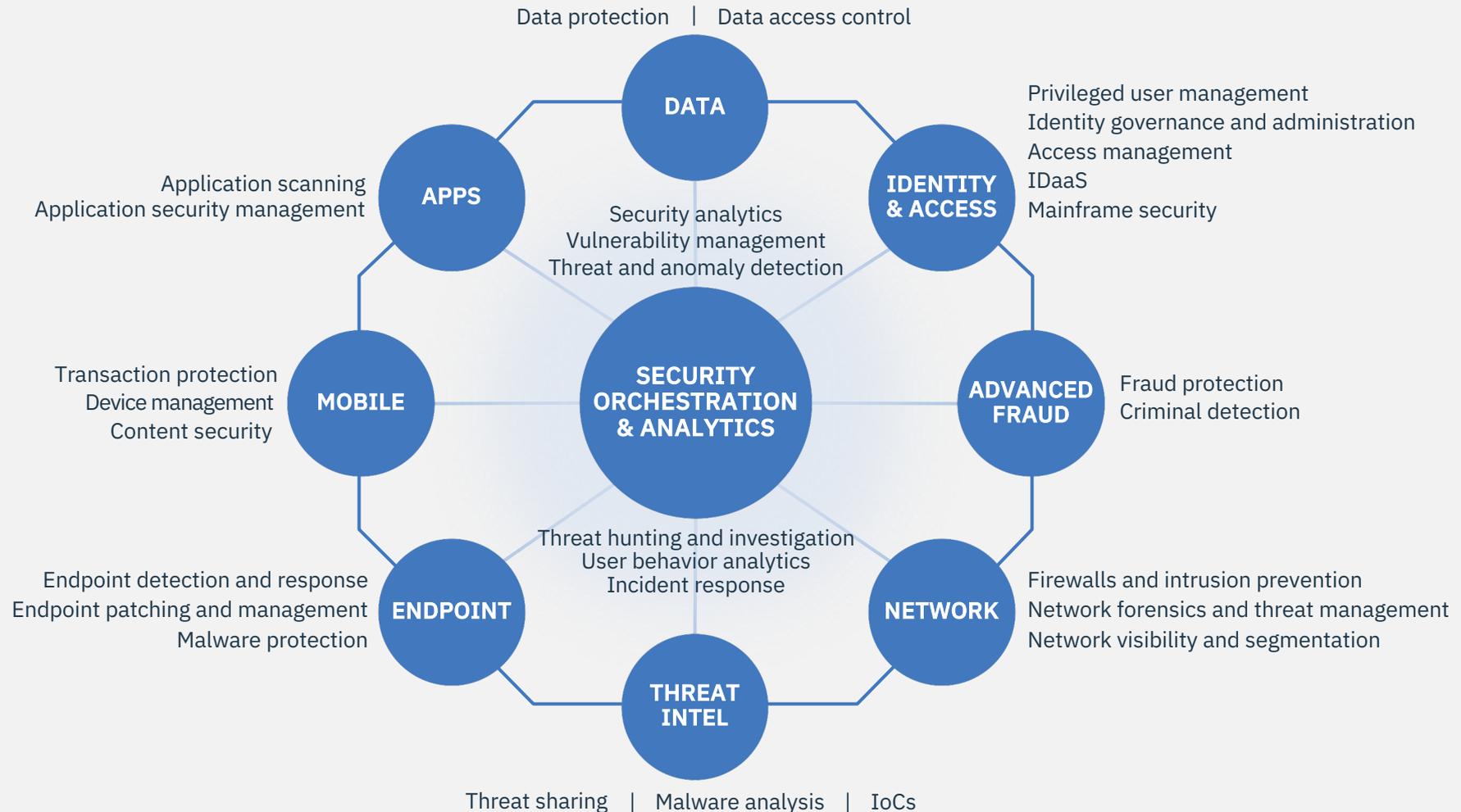
Malware analysis

Threat and anomaly detection

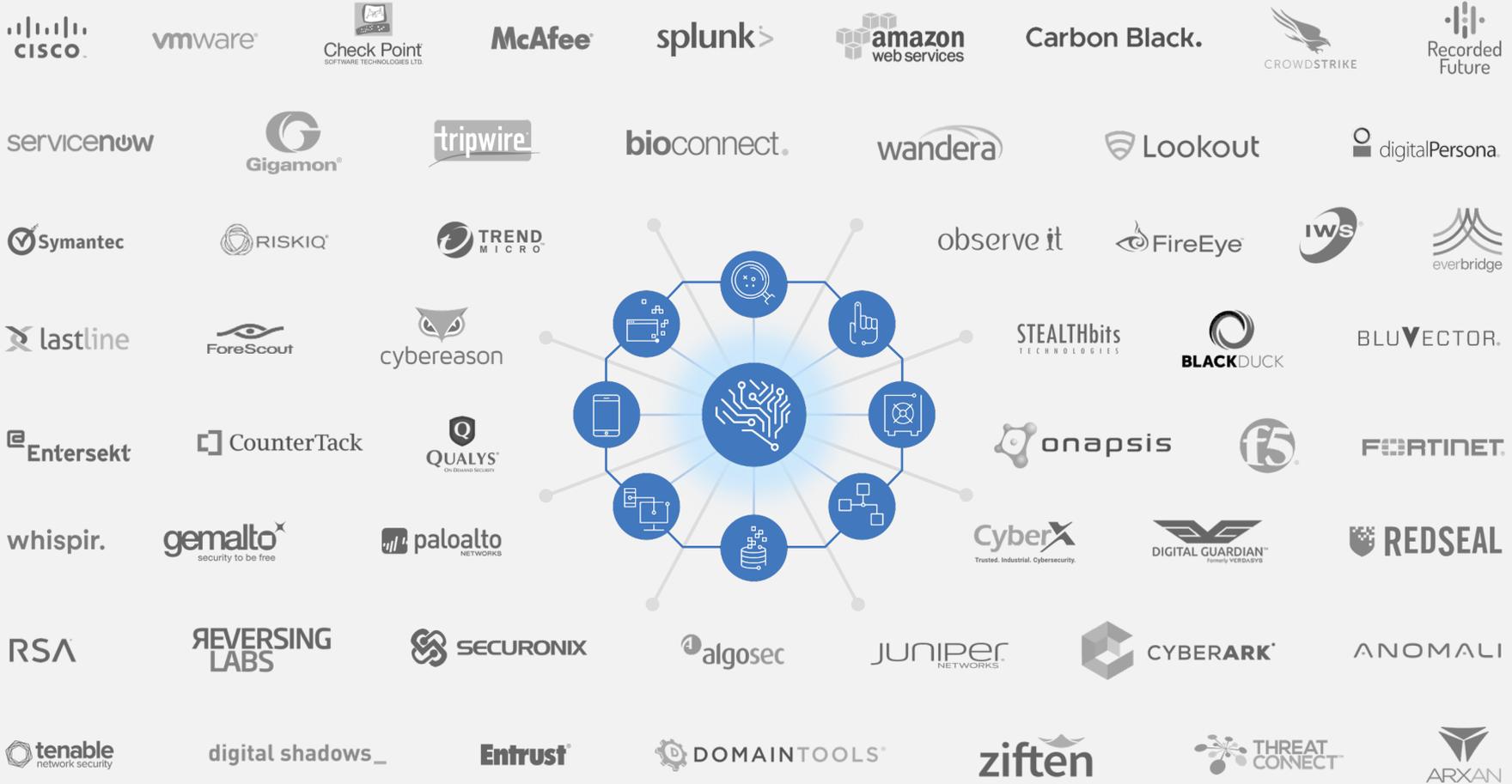
Application security management

Threat hunting and investigation

# Build an integrated security immune system

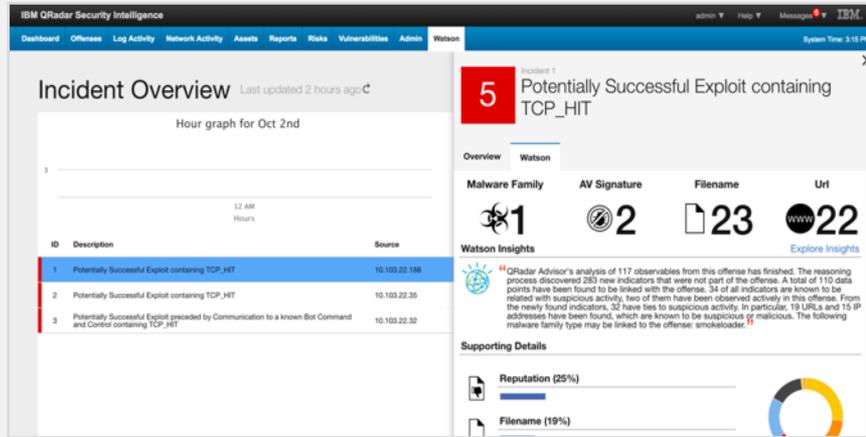


# Supported by hundreds of open integrations



# The future of security is AI and Orchestration

What if you could augment your teams' intelligence and response?

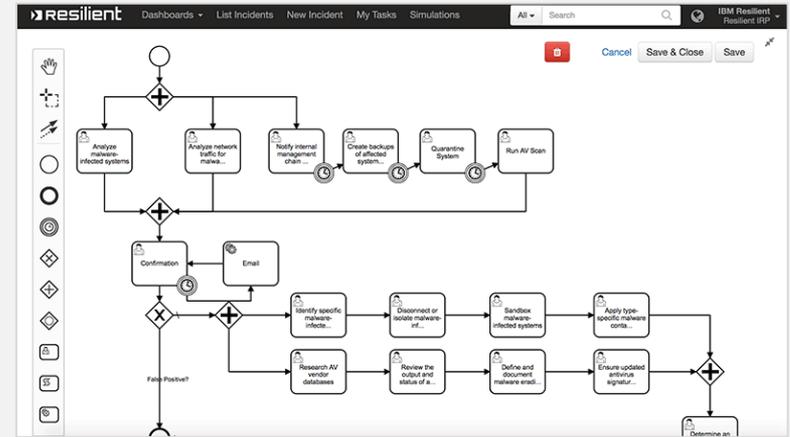


## Use AI to gain a head start

Automatically investigate incidents and anomalies to identify the most likely threats

- Quickly gather insights from millions of external sources
- Apply cognitive reasoning to build relationships

IBM QRadar Advisor with Watson



## Respond quickly with confidence

Orchestrate a complete and dynamic response, enabling faster, more intelligent remediation

- Create dynamic playbooks built on NIST / CERT / SANS
- Deploy response procedures and expertise

IBM Resilient

# The future of security is Collaboration

Are you part of the bigger picture?

Search by Application

All Applications (67) Sort By [dropdown]

- QRadar QRadar Advisor With Watson** (PREMIER)  
Enrich security incidents with insights from Watson to rapidly respond to threats.  
By IBM Security, IBM Validated
- QRadar User Behavior Analytics for QRadar** (UPDATED)  
IBM QRadar User Behavior Analytics app helps detect insider threat and malicious behaviors of...  
By IBM QRadar, IBM Validated
- QRadar Snare Log Analysis**  
The Snare Log Analysis QRadar application is designed to provide an overview dashboard of Snare...  
By Intersect Alliance I..., IBM Validated
- X-Force Exchange IBM X-Force Exchange SDK**  
The IBM X-Force Exchange SDK provides a powerful and extensible API for data processing, analysis...  
By IBM X-Force Exchange, IBM Validated
- QRadar IBM Resilient QRadar Integration**  
Integrate IBM Resilient with IBM QRadar to simplify and streamline the process of escalating and...  
By IBM, IBM Validated
- QRadar STEALTHbits Active Directory App for...**  
QRadar-based Active Directory Security Monitoring for Security Intelligence Professionals  
By STEALTHbits Technolo..., IBM Validated
- QRadar Palo Alto Networks App for QRadar**  
Reduce, prioritize, and correlate security events and leverage offense workflows to enable...  
By Palo Alto Networks, IBM Validated
- BigFix BigFix and Carbon Black Integration**  
Integration of BigFix with Carbon Black Enterprise solution provides advanced security management.  
By IBM, IBM Validated

Search [AlertCon™ Threat Level 1]

Search by Application name, IP, URL, Vulnerability, MD5.

Current Threat Activity

Country	Count	Category
Ecuador	186,344,230	Spam, Dynamic IPs
Colombia	190,253,187,144	Spam, Dynamic IPs
Tunisia	197,27,87,111	Spam, Dynamic IPs
Morocco	41,143,58,200	Spam, Dynamic IPs
Argentina	186,56,134,65	Spam, Dynamic IPs
Russia	77.1	Spam

Malicious IP addresses in the last hour

Category	Count
Command and Control	1
Spam	1,266
Malware	47
Scanning	55

Join an ecosystem of defenses

Customize your security with 140+ apps on the [IBM Security App Exchange](#)

Share real-time threat intelligence

Interact with 41K+ users and 800+ TB of threat intelligence on the [IBM X-Force Exchange](#)

A person is seen from behind, looking at a row of computer monitors in a dimly lit room. The monitors display various security-related graphics, including shields and data charts. The overall atmosphere is dark and focused, with blue and red lighting accents.

# FIGHT THREATS

“We need help analyzing huge amounts of information in real-time to identify trends and useful information for more actionable insights.”



**Detect & Stop  
Advanced Threats**



**Orchestrate  
Incident Response**



**Master  
Threat Hunting**

# Detect and stop advanced threats

IBM QRadar Security Intelligence

admin Help Messages 6 IBM

Dashboard Offenses Log Activity Network Activity Assets Reports Risks Vulnerabilities Admin Watson System Time: 3:15 PM

## Incident Overview Last updated 2 hours ago

Hour graph for Oct 2nd

ID	Description	Source
1	Potentially Successful Exploit containing TCP_HIT	10.103.22.188
2	Potentially Successful Exploit containing TCP_HIT	10.103.22.35
3	Potentially Successful Exploit preceded by Communication to a known Bot Command and Control containing TCP_HIT	10.103.22.32

Incident 1

### 5 Potentially Successful Exploit containing TCP\_HIT

Overview Watson

Malware Family	AV Signature	Filename	Url
1	2	23	22

Watson Insights [Explore Insights](#)

“QRadar Advisor’s analysis of 117 observables from this offense has finished. The reasoning process discovered 283 new indicators that were not part of the offense. A total of 110 data points have been found to be linked with the offense. 34 of all indicators are known to be related with suspicious activity, two of them have been observed actively in this offense. From the newly found indicators, 32 have ties to suspicious activity. In particular, 19 URLs and 15 IP addresses have been found, which are known to be suspicious or malicious. The following malware family type may be linked to the offense: smokeloader.”

Supporting Details

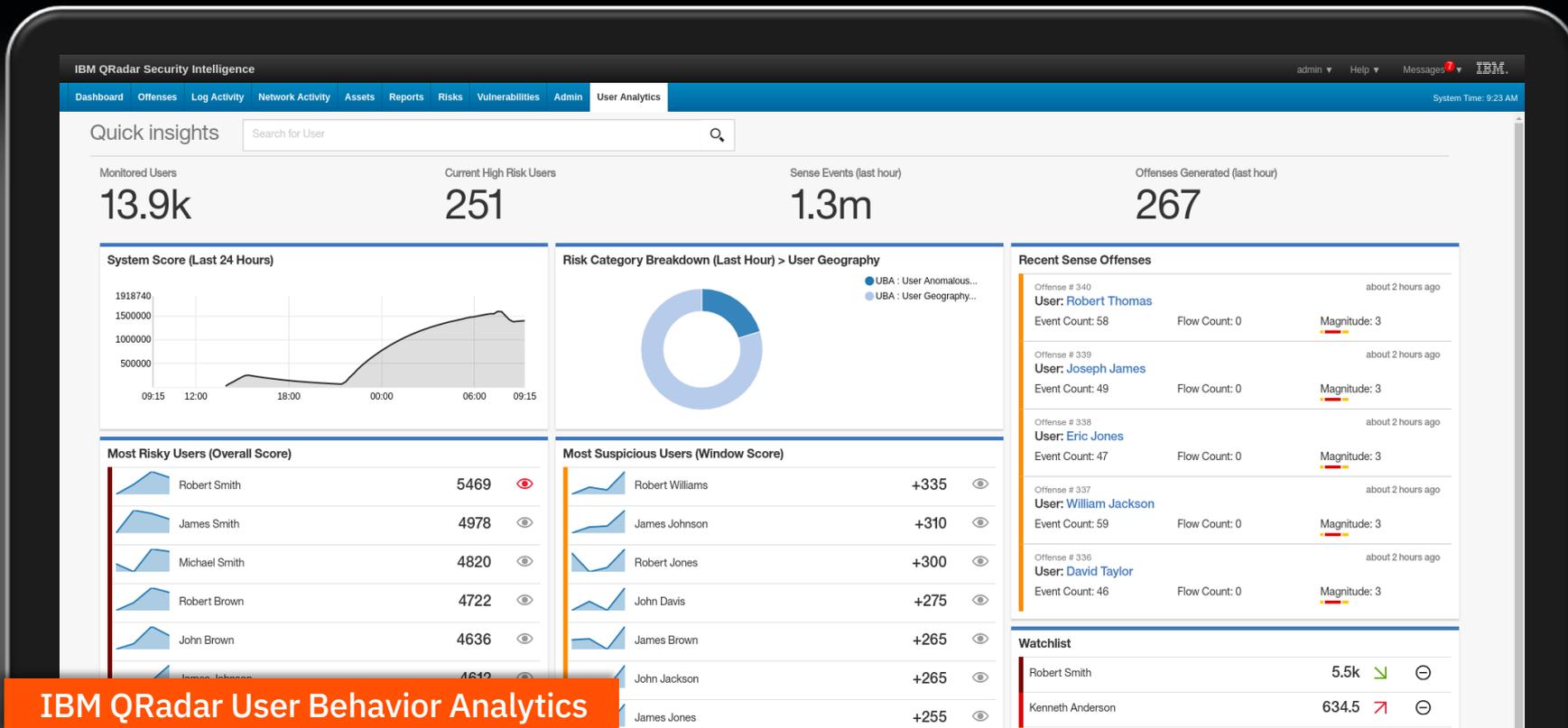
Reputation (25%)

## IBM QRadar Advisor with Watson

Automatically uncover the full scope of a security incident

- **2.3M+** security documents
- **80K+** documents read per day
- **10B+** security data elements
- **250K+** investigations enhanced

# Detect and stop advanced threats



## IBM QRadar User Behavior Analytics

Advanced analytics for advanced threat detection and response across the enterprise

The User Behavior Analytics dashboard is an integrated part of the QRadar console

# Orchestrate incident response

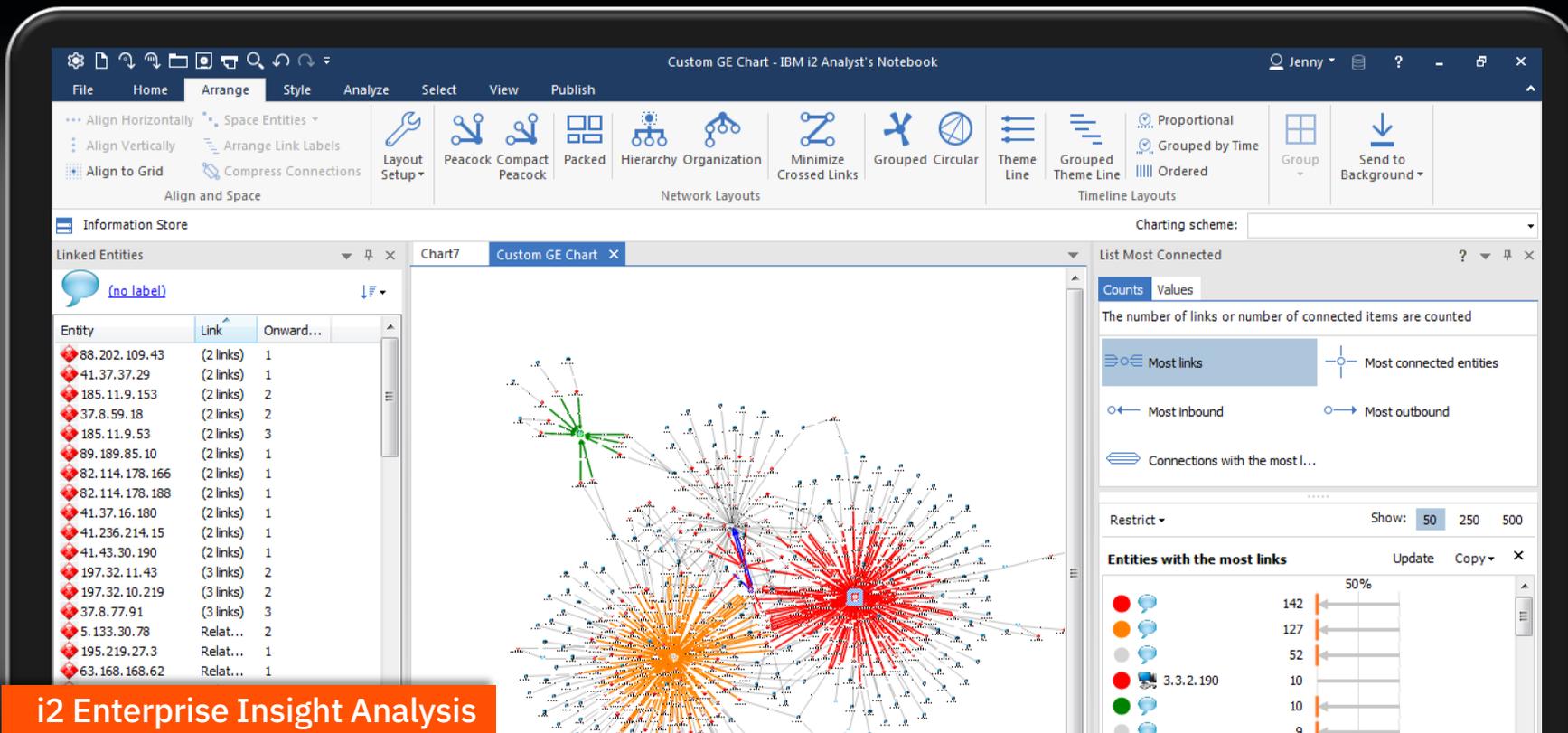
The screenshot displays the IBM Resilient interface for incident response. At the top, there is a navigation bar with the 'resilient' logo, 'Dashboards', 'List Incidents' (selected), 'New Incident', 'My Tasks', 'Simulations', and a search bar. The user 'Adam Koblentz' is logged in. The main content area shows incident details: Severity: High, Date Created: 07/13/2016, Date Occurred: —, Date Discovered: 07/13/2016, Data Compr.: Yes, Incident Type: Malware, Destination Network: Net-10-172-192.Net\_192\_168\_0\_0, Protocol: other(255), and QID: 28250184. Below the details is a tabbed interface with 'News Feed' selected. The 'News Feed' shows three entries: 1. 'Marc Makowski wrote a note on the task Initial Triage' with a quote from Carlo Alpuerto: 'Can you finish today?'. 2. 'Marc Makowski reassigned task Notify internal management chain (preliminary)'. 3. 'Zach Taira added a row to the Data Table Task History'. On the left, there is a 'People' section listing 'Created By: Tim Armstrong', 'Owner: Zach Taira', and 'Members: Carlo Alpuerto, Jody Cannady, Ethan Goldstein'. Below that is a 'Related Incidents' section with a link to '#3852 Proofpoint Sample Alert 34342'.

## IBM Resilient Incident Response

End-to-end workflow, collaboration, actions and expertise to respond with confidence

- Hunt for indicators using deep forensics
- Deploy response procedures and expertise

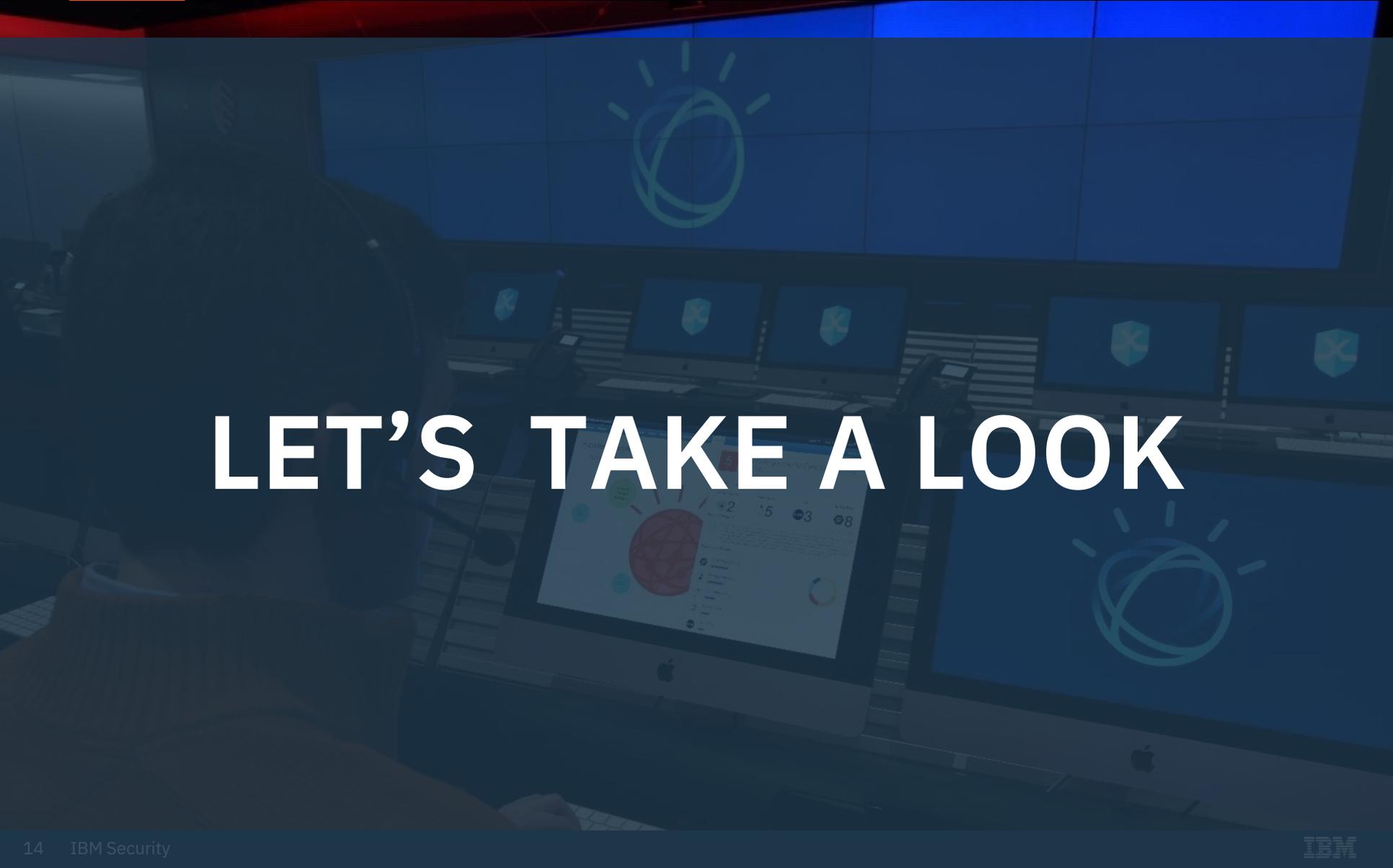
# Master threat hunting



## i2 Enterprise Insight Analysis

Analyst-driven investigations using big data and threat intelligence to get ahead of the threats

- Visually investigate with built-in analytics to uncover hidden threats faster
- Easily combine both structured and unstructured data to support investigative analysis

A person is seen from behind, looking at a large array of computer monitors in a dimly lit room. The monitors display various data visualizations, including a globe and charts. The room is illuminated with blue light, and a stylized sun icon is visible on the wall behind the monitors. The text "LET'S TAKE A LOOK" is overlaid in the center of the image.

**LET'S TAKE A LOOK**



# THANK YOU

## FOLLOW US ON:

 [ibm.com/security](https://ibm.com/security)

 [securityintelligence.com](https://securityintelligence.com)

 [ibm.com/security/community](https://ibm.com/security/community)

 [xforce.ibmcloud.com](https://xforce.ibmcloud.com)

 [@ibmsecurity](https://twitter.com/ibmsecurity)

 [youtube.com/user/ibmsecuritysolutions](https://youtube.com/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2018. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.