IBM Security

Integrované nástroje v modernom centre bezpečnostných operácií

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

April 2018

IBM

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

Identity governance and administration

Network visibility and segmentation

Fraud protection

Mainframe security

Network forensics and threat management

Application scanning

Vulnerability management

Malware protection

IDaaS

Device management

IoCs

Threat sharing

Endpoint detection and response

Transaction protection

Criminal detection

Content security

Malware analysis

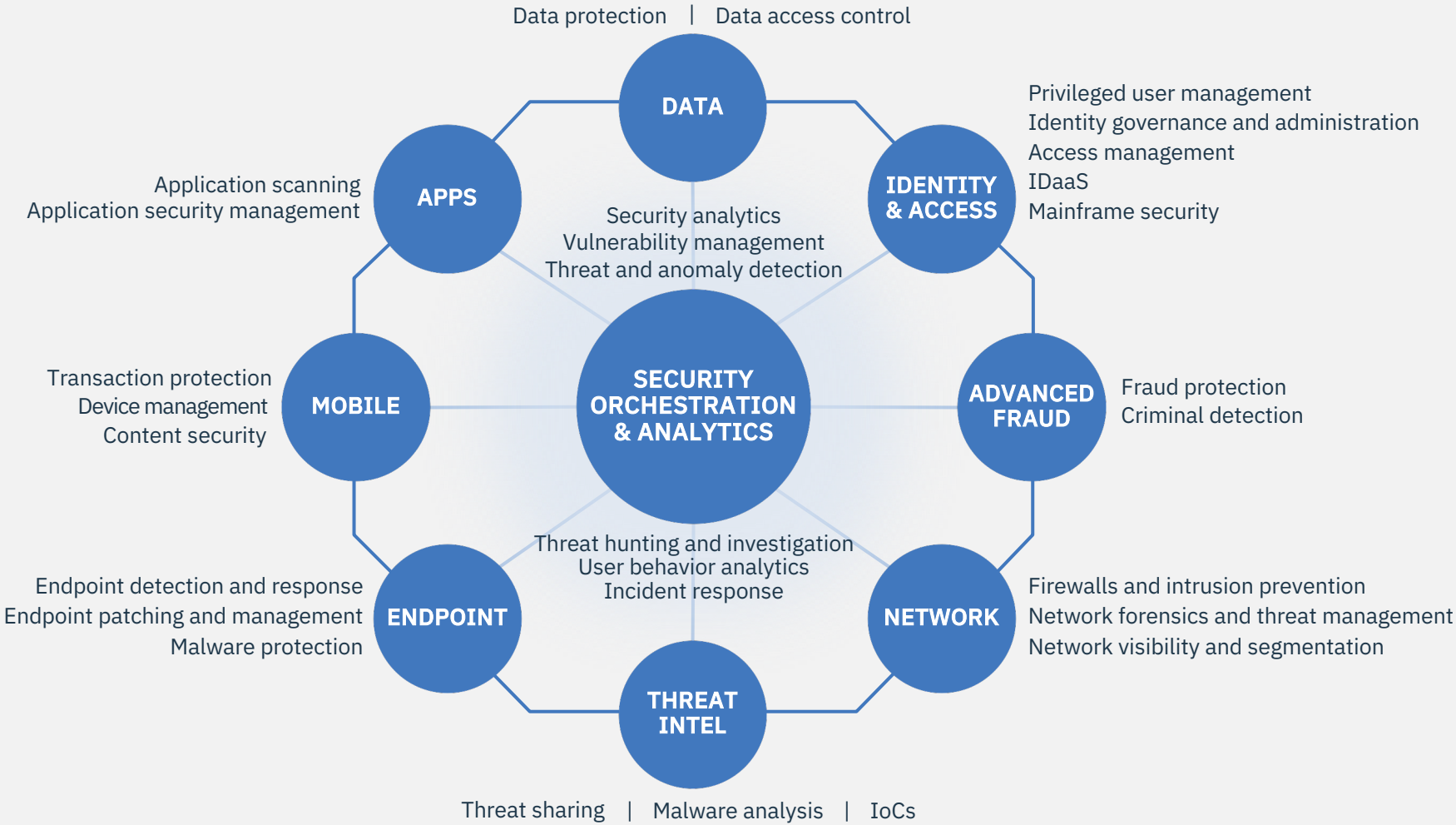
Firewalls and intrusion prevention

Threat and anomaly detection

Application security management

Threat hunting and investigation

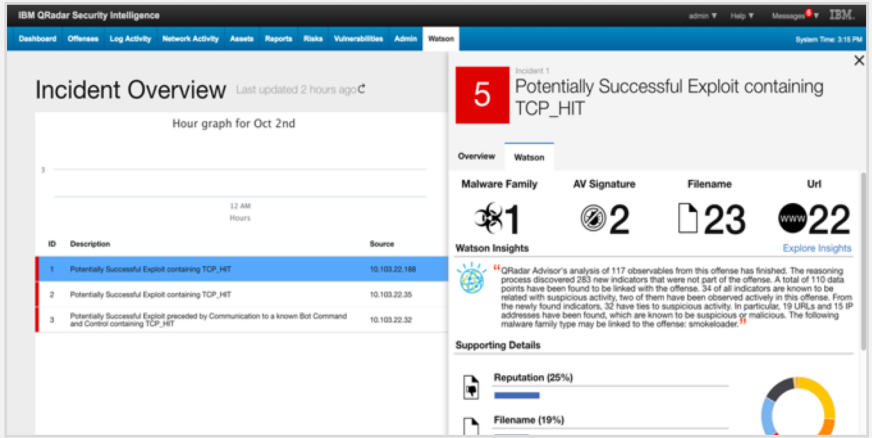
Build an integrated security immune system

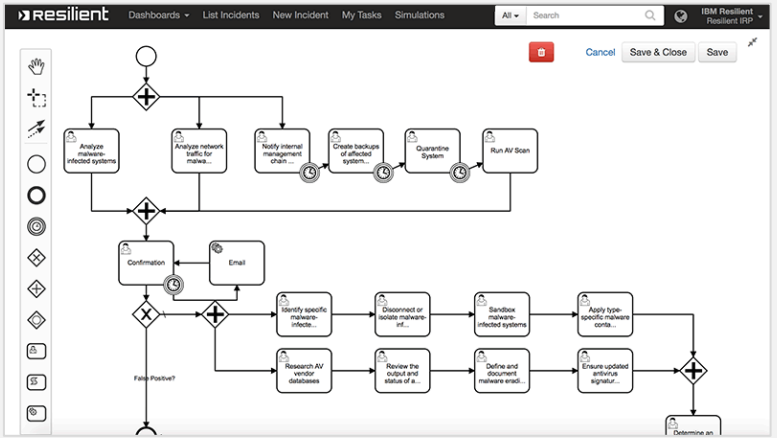


Supported by hundreds of open integrations

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

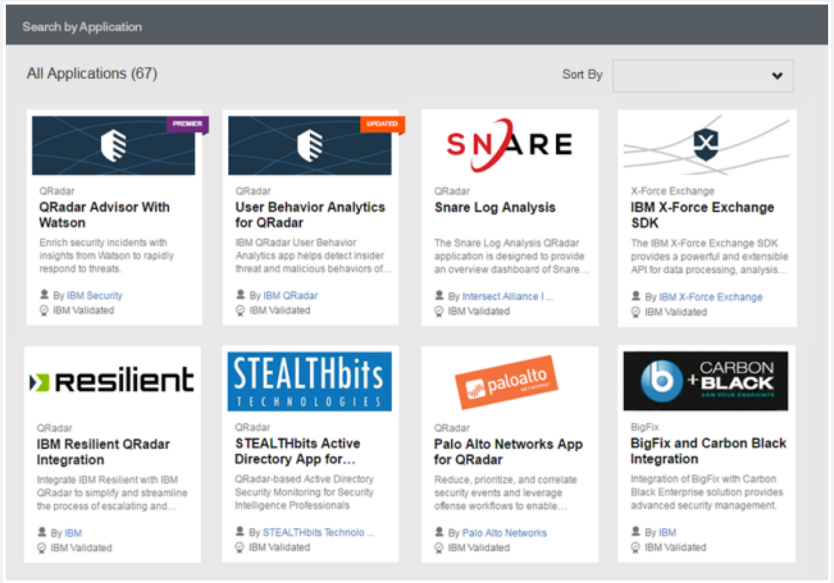
Orchestrate a complete and dynamic response, enabling faster, more intelligent remediation

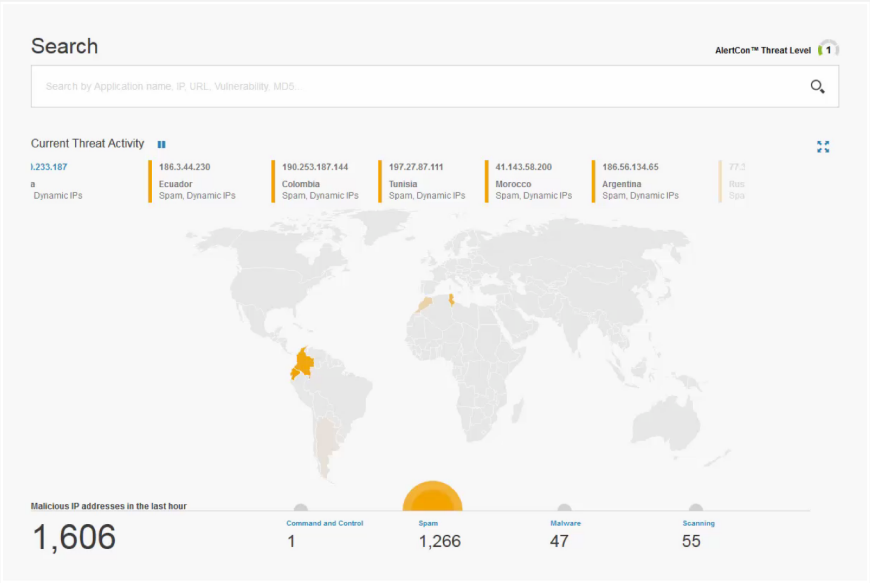
- Create dynamic playbooks built on NIST / CERT / SANS
- Deploy response procedures and expertise

IBM Resilient

The future of security is Collaboration

Are you part of the bigger picture?





Join an ecosystem of defenses

Customize your security with 140+ apps on the IBM Security App Exchange

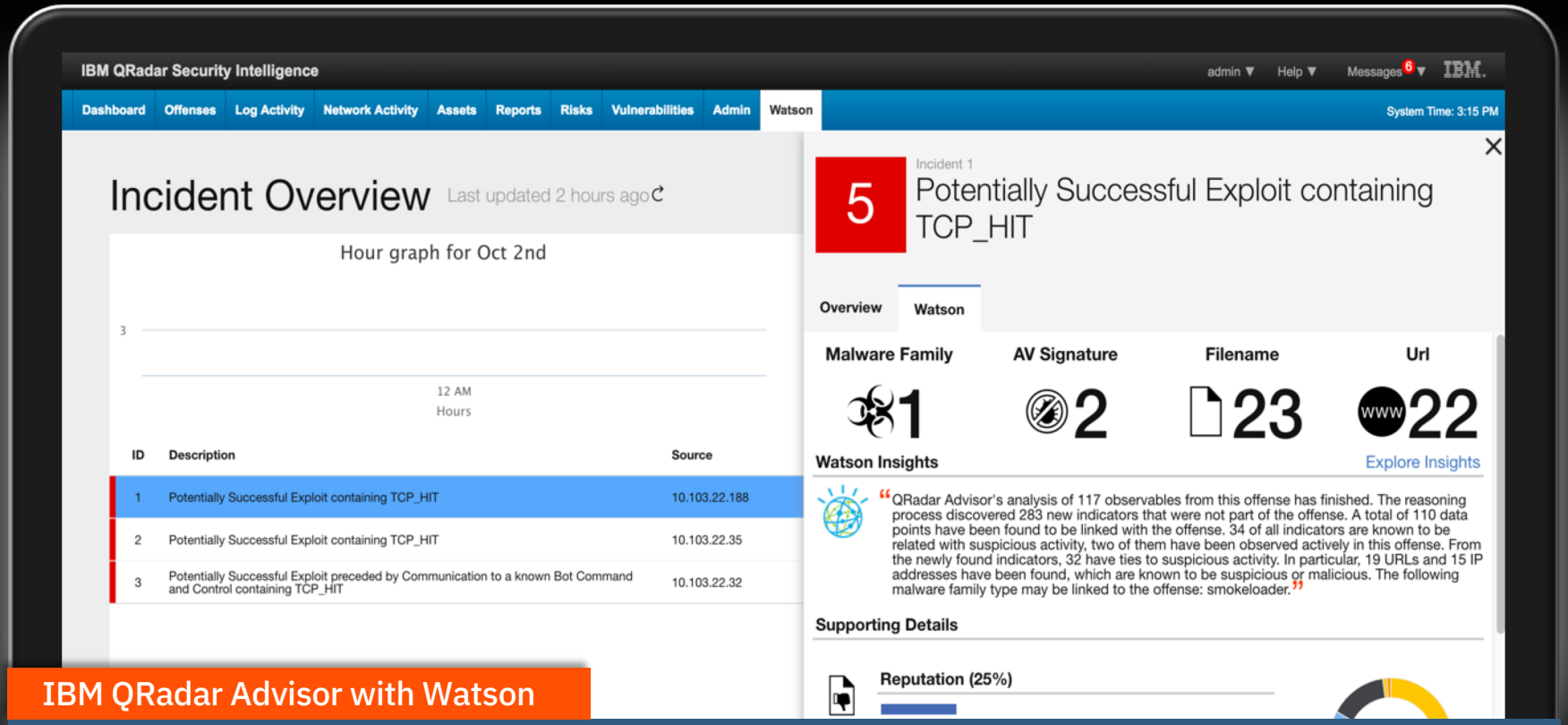
Share real-time threat intelligence

Interact with 41K+ users and 800+ TB of threat intelligence on the IBM X-Force Exchange


FIGHT THREATS

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

Detect and stop advanced threats

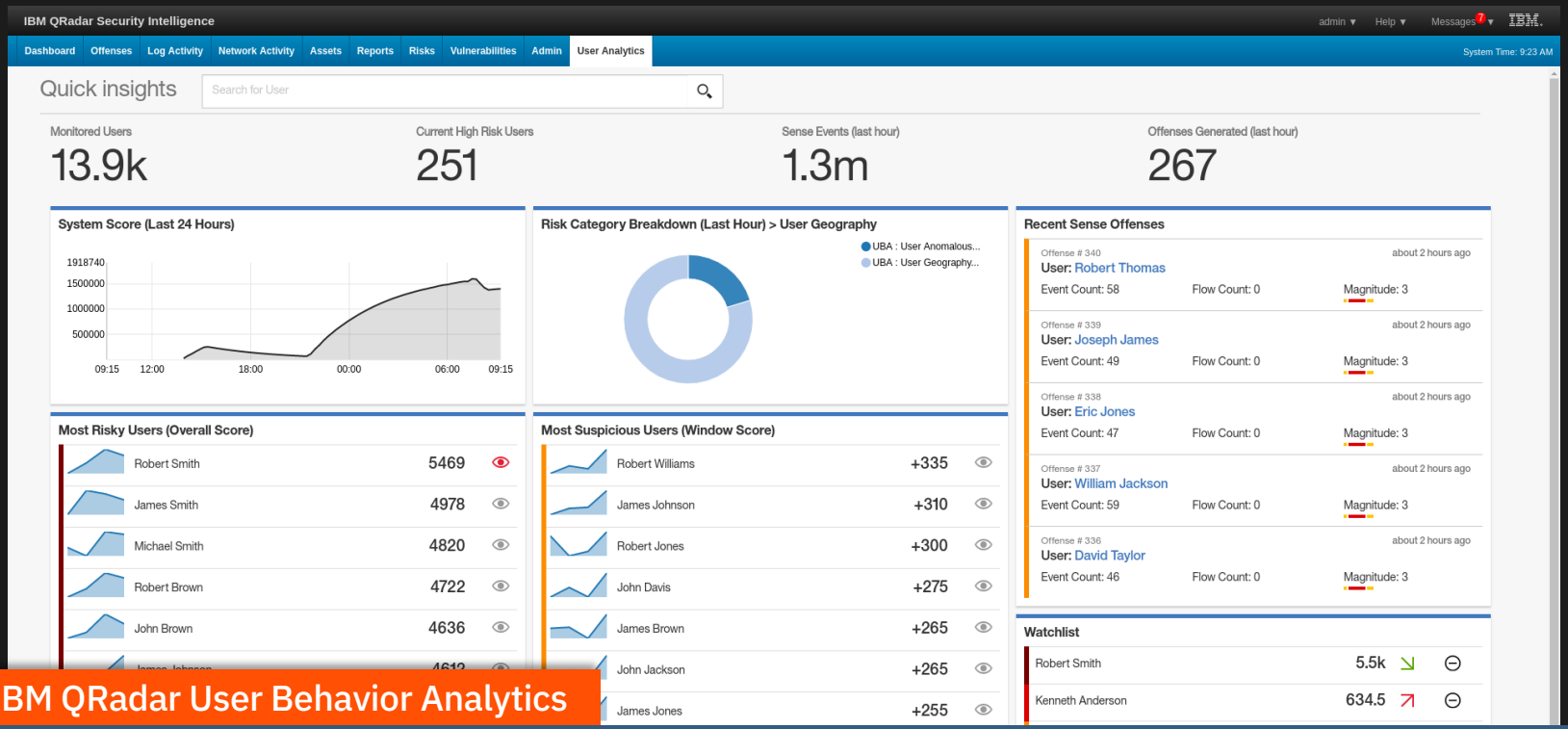


IBM QRadar Advisor with Watson

Automatically uncover the full scope of a security incident

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

Detect and stop advanced threats

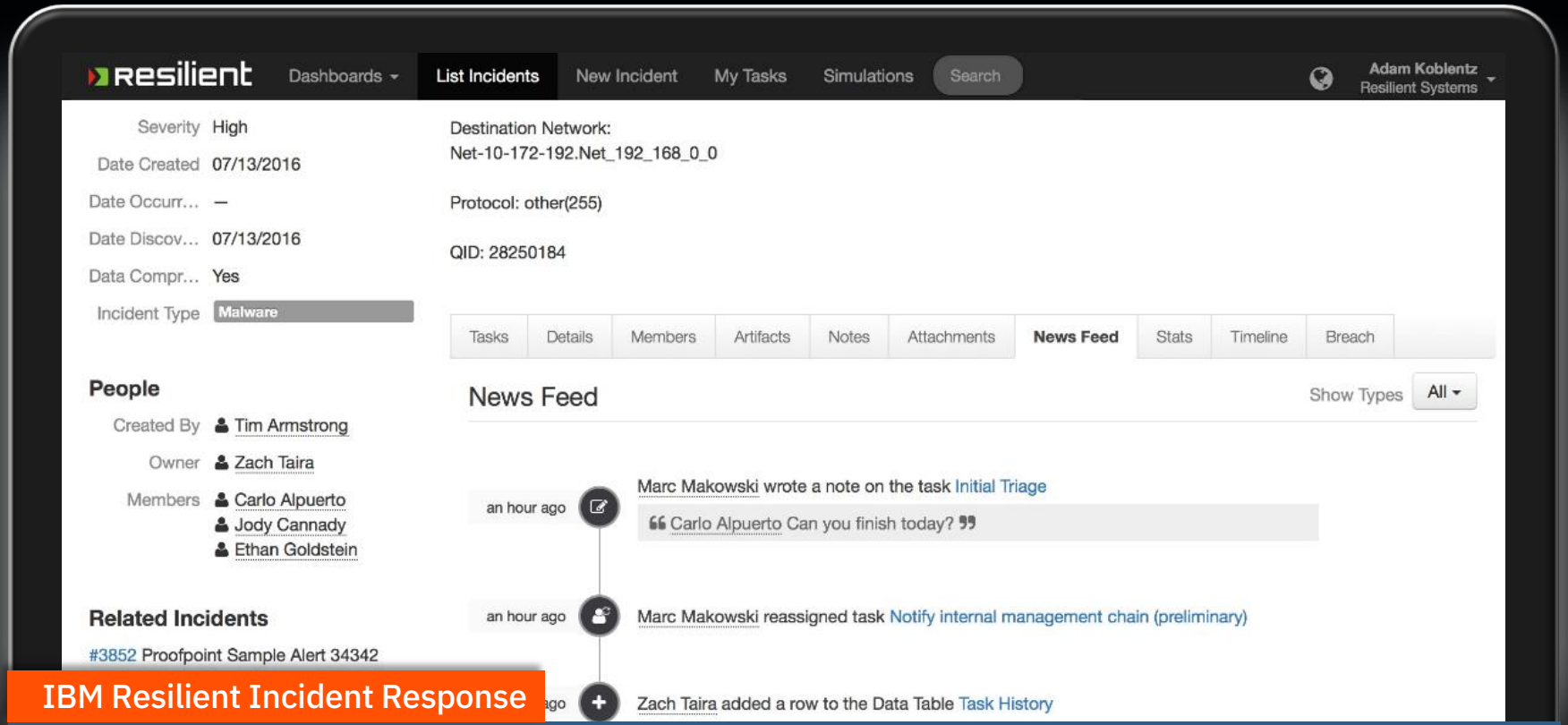


IBM QRadar User Behavior Analytics

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

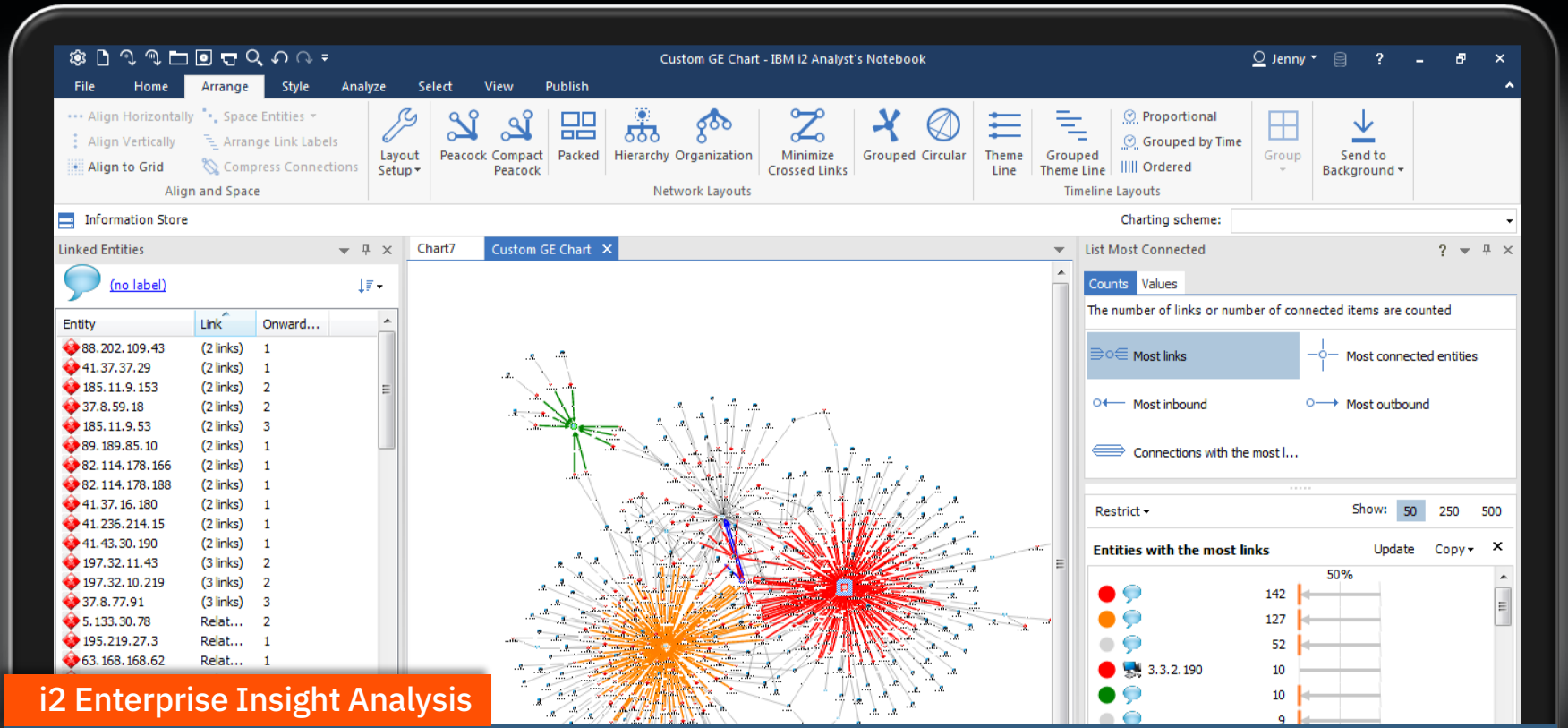


IBM Resilient Incident Response

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

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

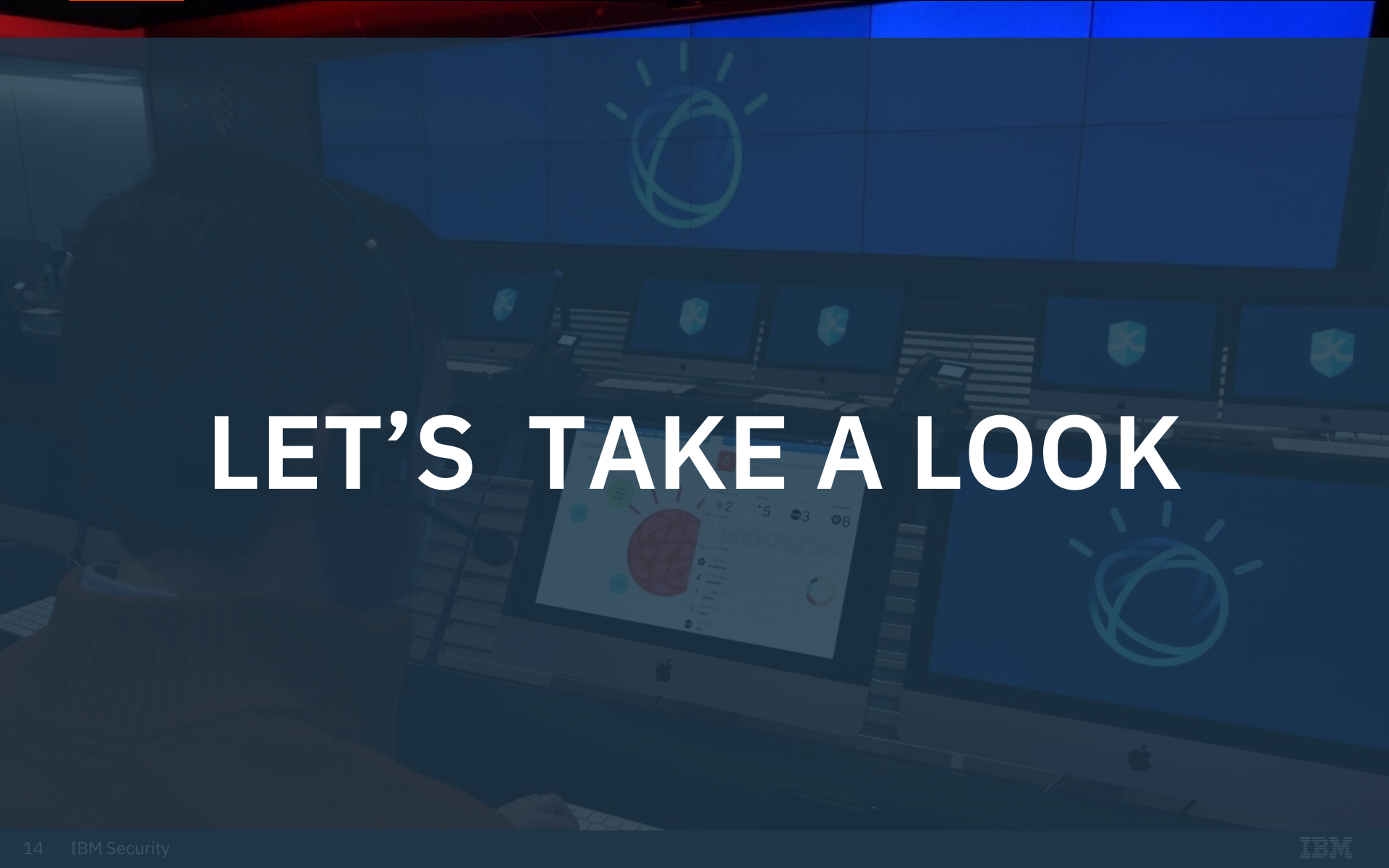
Master threat hunting



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


LET’S TAKE A LOOK

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

IBM