IBM Security

Security Information View in Relation to New Technologies

SECURITY FOR A NEW ERA OF COMPUTING

Jeff Crume, CISSP-ISSAP
Distinguished Engineer
IBM Master Inventor
IT Security Architect
crume@us.ibm.com
Blog: InsideInternetSecurity.com

IBM

Today’s security drivers

Three key security technology trends

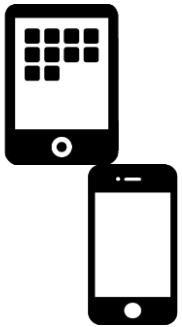
- Risk Based Access
- Security Information Sharing
- Cognitive Security

Landscape of Identity & Access Management market is evolving

By 2020,

70%

of enterprises will use **attribute-based access control** as the dominant mechanism to protect critical assets ...



... and

80%

of user access will be shaped by **new mobile and non-PC architectures** that service all identity types regardless of origin.[1]

With the growing adoption of mobile, adaptive authentication & fine-grained authorization, traditional Web Access Management is being replaced by a broader "access management."[1]

A clear need exists in the market for a converged solution[2] that is able to provide or integrate with MDM, authentication, federation, and fraud detection solutions.[3]

1 Gartner, *Predicts 2014: Identity and Access Management,* November 26, 2013
2 Gartner, *MarketScope for Web Access Management,* November 15, 2013
3 Forrester, *Predictions 2014: Identity and Access Management,* January 7, 2014

Can we leverage this trend for better security?

Multi-Factor Authentication and Risk Based Access

Authentication options*

*** Stronger authentication may be effective in mitigating userid/password credential compromise; advanced malware/RAT can circumvent many in-band multi-factor mechanisms**

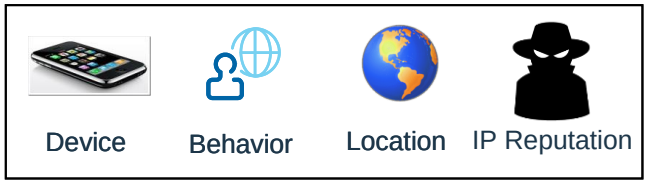

Password


SMS


Phone


Biometric

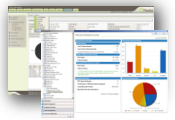

Code Generation

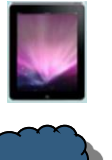


Utilizing a variety of factors/policies (e.g. device detection, location, etc.) client identity is authenticated outside of LoB environment

Multiple factors are used from the login context to assess the risk and determine if stronger authentication is required.


Device Registry, User History






Web Access Gateway

Authorization Service

Risk Engine
Assess Risk Score

Authentication Service

Authorization Policy:

If AUTHLEVEL = password and RISK_SCORE > 40 then permit wth OTP

If AUTHLEVEL = password and RISK_SCORE < 40 then permit

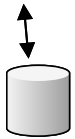
If AUTHLEVEL = OTP and RISK_SCORE >80 then deny

If AUTHLEVEL = password and XACT_AMT > $10000 then permit with OTP

Cloud Partners

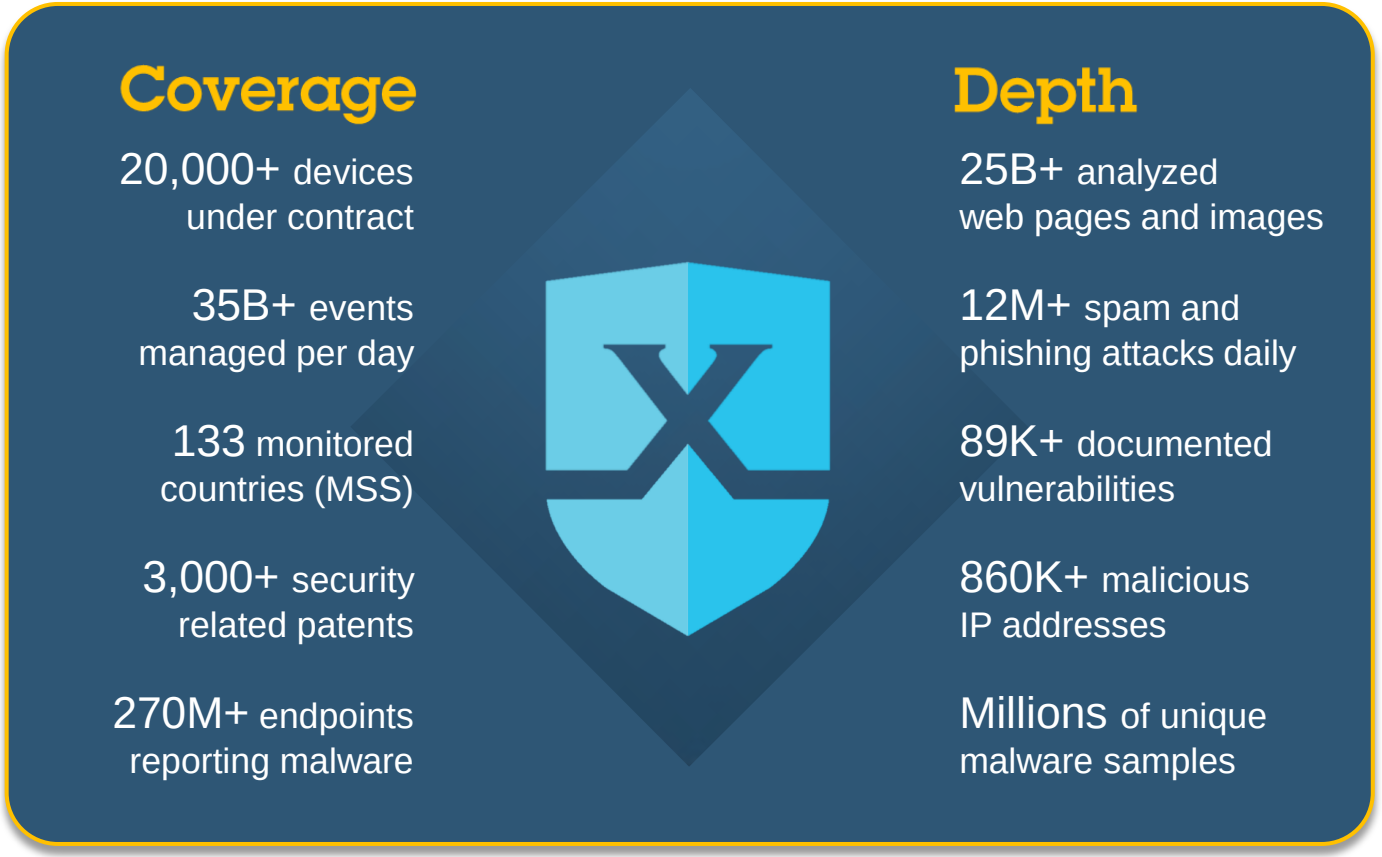
The user has an opportunity to use a variety of devices to access LoB apps including mobile & regular browsers.


Application Servers


User Registry

Security Information Sharing

IBM X-Force monitors and analyzes the changing threat landscape



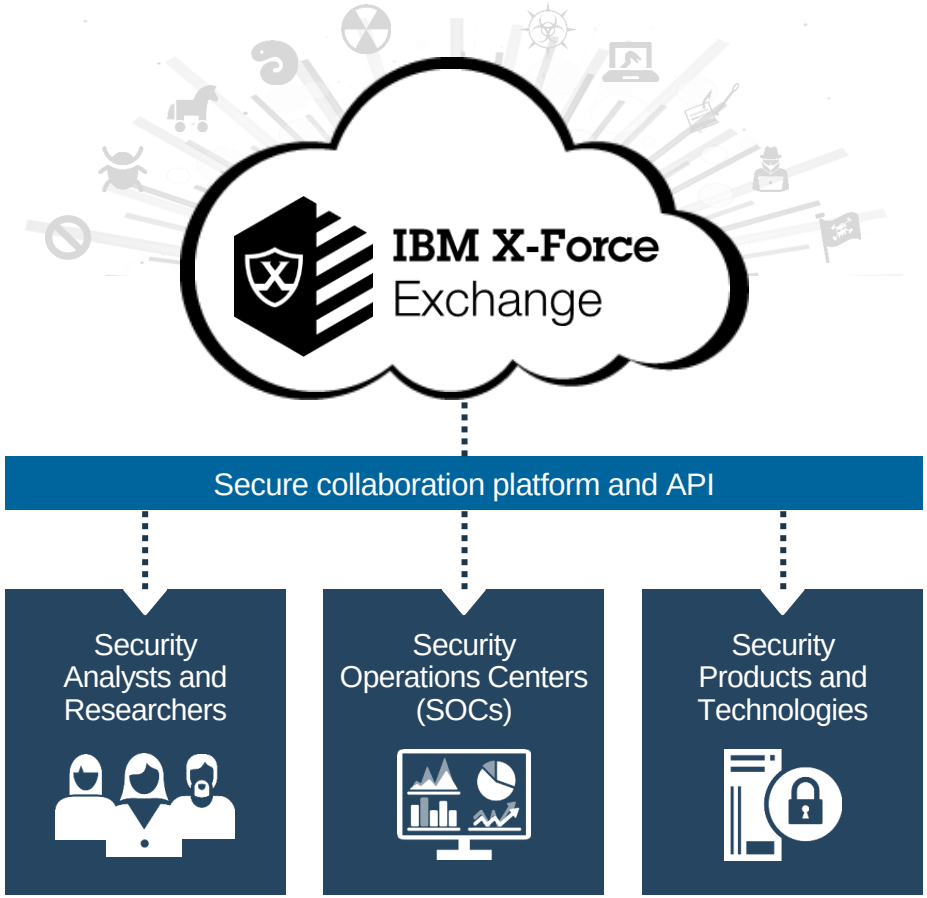
IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape

The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

IBM X-Force Exchange



A new platform to consume, share, and act on threat intelligence

IBM X-Force Exchange is:

TRUSTED
a robust and secure platform built by one of the most trusted global brands

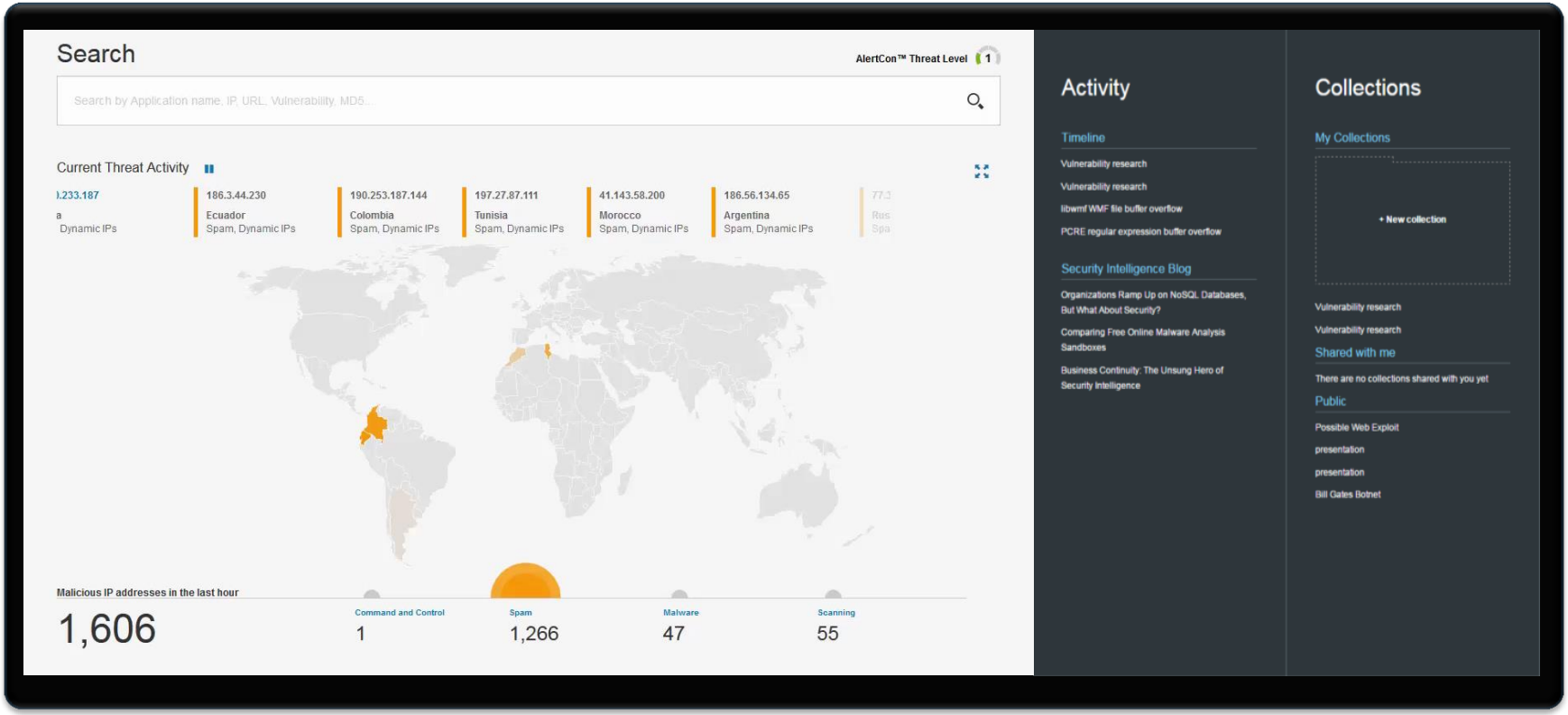
SOCIAL
a collaborative platform for sharing threat intelligence

ACTIONABLE
an integrated solution to help quickly stop threats

Backed by the reputation and scale of one of the most recognized security research teams in the world

Collaboration

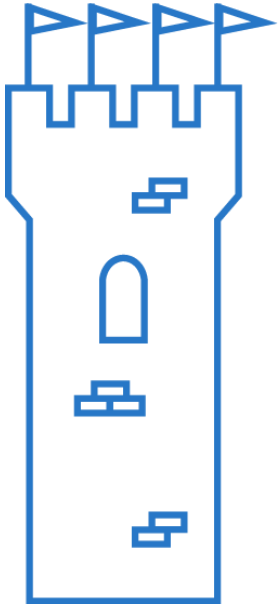
Crowd-sourced information sharing based on 700+TB of threat intelligence



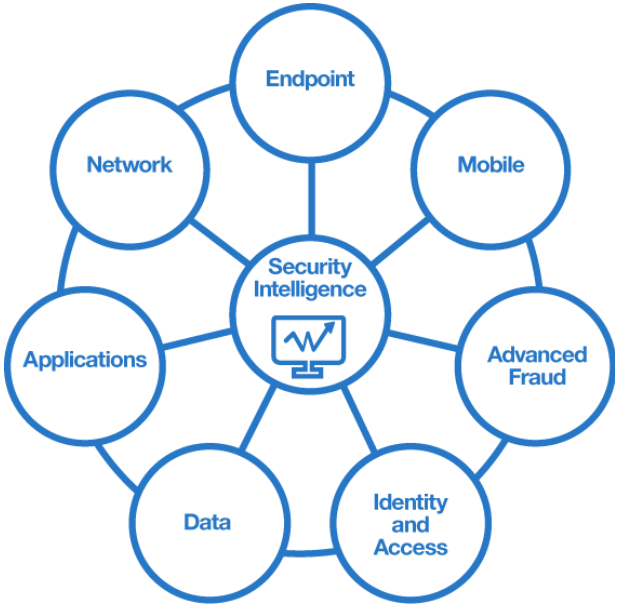
https://exchange.xforce.ibmcloud.com

Cognitive Security

The next era of security



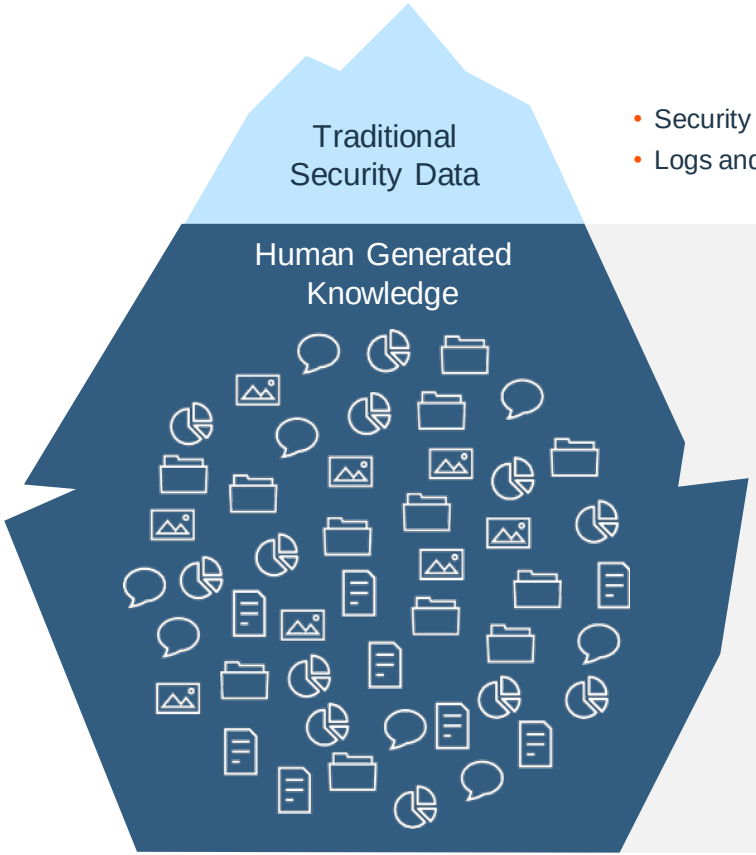
Moats, Castles



Intelligence, Integration

Cloud, Collaboration, Cognitive

A tremendous amount of security knowledge is created for human consumption, but most of it is untapped



- Security events and alerts
- Logs and configuration data
- User and network activity
- Threat and vulnerability feeds

A universe of security knowledge Dark to your defenses

Typical organizations leverage only 8% of this content*

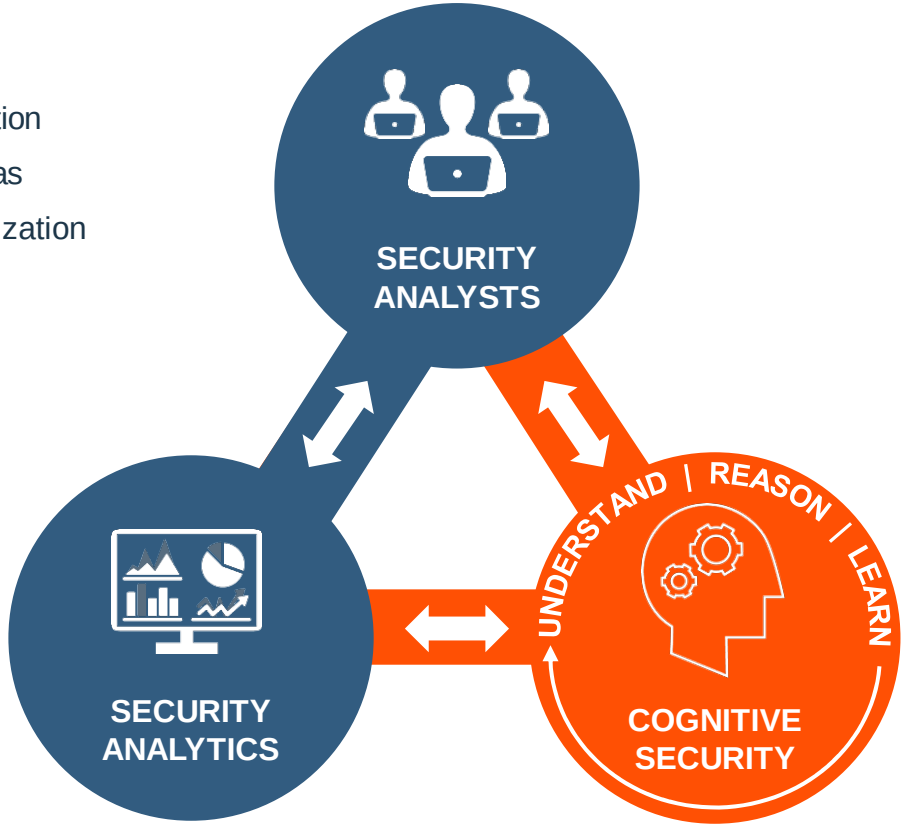
Examples include:

- Research documents
- Industry publications
- Forensic information
- Threat intelligence commentary
- Conference presentations
- Analyst reports
- Webpages
- Wikis
- Blogs
- News sources
- Newsletters
- Tweets

Cognitive systems bridge this gap and unlock a new partnership between security analysts and their technology

Human Expertise

- Common sense
- Morals
- Compassion
- Abstraction
- Dilemmas
- Generalization



Security Analytics

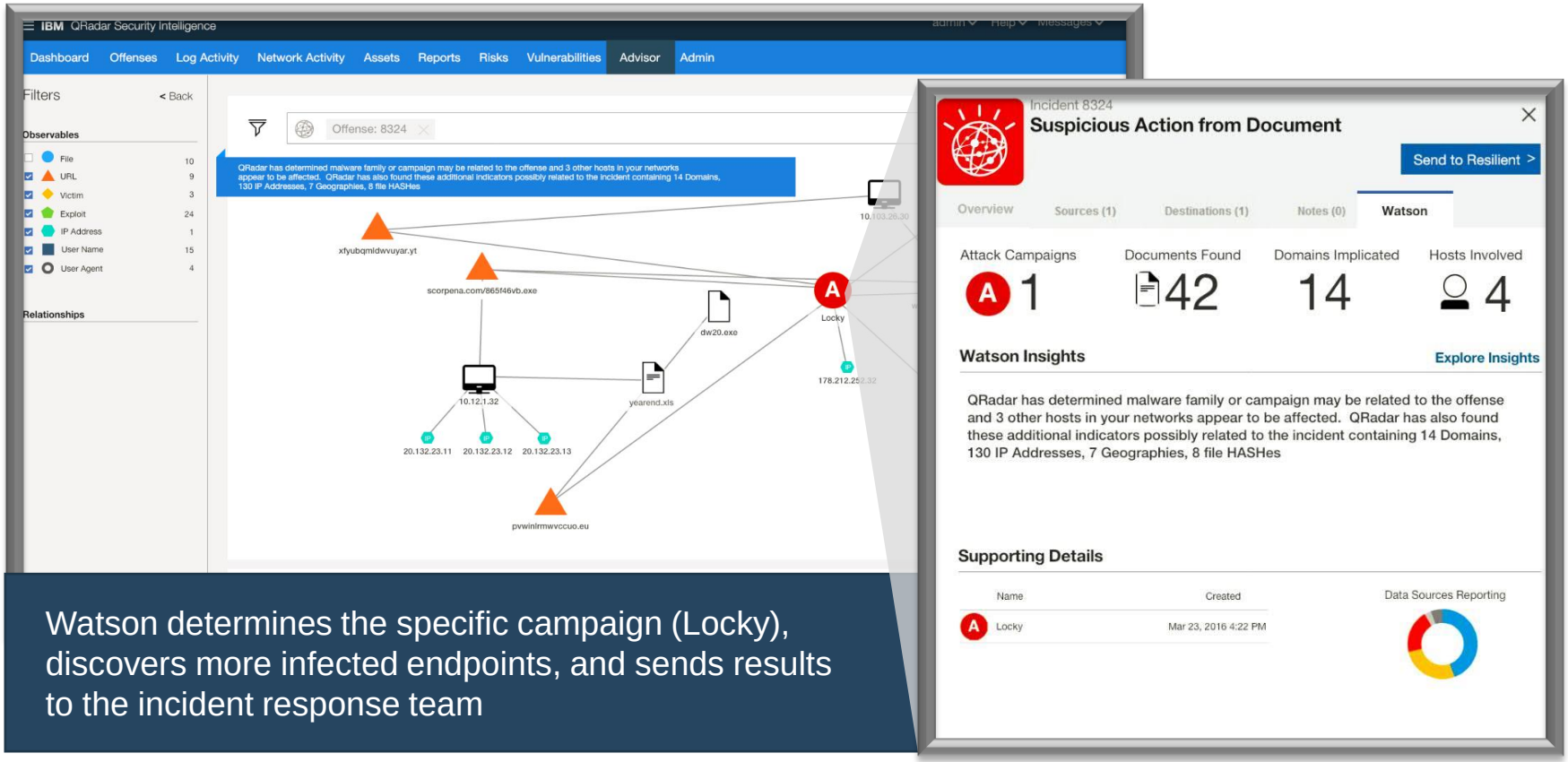
- Data correlation
- Pattern identification
- Anomaly detection
- Prioritization
- Data visualization
- Workflow

Cognitive Security

- Unstructured analysis
- Natural language
- Question and answer
- Machine learning
- Bias elimination
- Tradeoff analytics

Cognitive: Revolutionizing how security analysts work

Natural language processing with security that understands, reasons, and learns



Watson determines the specific campaign (Locky), discovers more infected endpoints, and sends results to the incident response team

IBM Security

THANK YOU

FOLLOW US ON:

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

IBM