IBM Security
Intelligence. Integration. Expertise.

IBM

How to Choose the Right Security Information and Event Management (SIEM) Solution

John Burnham
Director, Strategic Communications and Analyst Relations
IBM Security

Chris Meenan
Director, Security Intelligence Product Management and Strategy
IBM Security

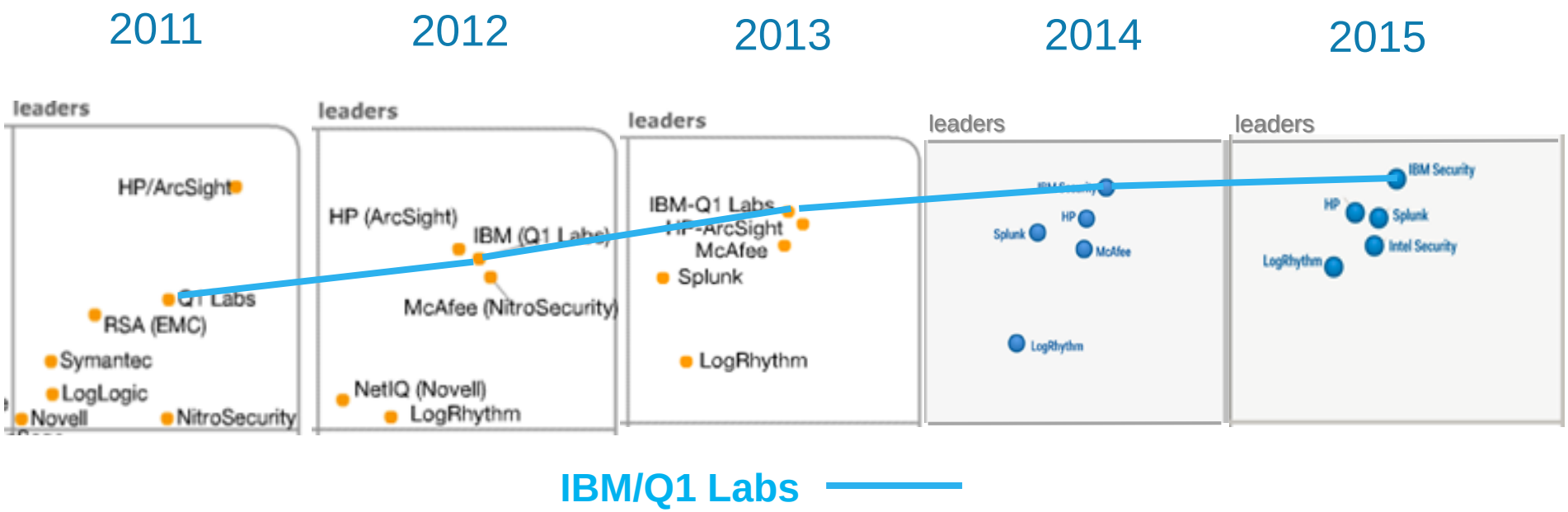
Agenda

- Introduction
- 2015 Gartner Magic Quadrant for SIEM
- IBM Security QRadar SIEM Solutions
  - How we got here

Agenda

- Introduction
- 2015 Gartner Magic Quadrant for SIEM
- IBM Security QRadar SIEM Solutions
  - How we got here

QRadar in Gartner MQ Leaders Quadrant over the last 5 years



IBM/Q1 Labs

- Vertical axis is “Ability to Execute
- Horizontal Axis is “Completeness of Vision”

IBM QRadar is in SIEM Leadership Quadrant For Seventh Straight Year

"Magic Quadrant for Security Information and Event Management," Gartner, July 2015

2015 Gartner MQ for SIEM:

IBM Security QRadar is highest on "Ability to Execute" (the Y-axis) AND furthest to the right on "Completeness of vision" (the X-axis)

- Ability to execute is an assessment of overall viability, product service, customer experience, market responsiveness, product track record, sales execution, operations, and marketing execution.
- Completeness of Vision is a rating of product strategy, innovation, market understanding, geographic strategy, and other factors
- *"The need for early detection of targeted attacks and data breaches is driving the expansion of new and existing SIEM deployments. Advanced users are looking to augment SIEM with advanced profiling and analytics."*

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose

IBM Security QRadar in Leadership Quadrant for Seventh Straight Year

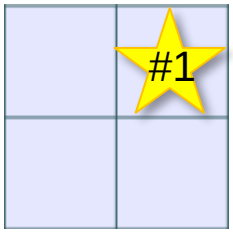
"Magic Quadrant for Security Information and Event Management," Gartner, July 2015

What Gartner is Saying about QRadar

- "Midsize and large enterprises with general SIEM requirements, and those with use cases that require behavior analysis, network flow and packet analysis, should consider QRadar."
- "Customer feedback indicates that the technology is relatively straightforward to deploy and maintain in both modest and large environments."
- "QRadar provides behavior analysis capabilities for NetFlow and log events."
- "The average of IBM reference customers satisfaction scores for scalability and performance, effectiveness of predefined correlation rules, report creation, ad hoc queries, product quality and stability, and technical support is higher than the average scores for all reference customers in those areas."

IBM Security QRadar in Leadership Quadrant for Seventh straight year

"Magic Quadrant for Security Information and Event Management," Gartner, July 2015



Other Gartner Comments about IBM Security QRadar:

- "IBM Security's QRadar Platform includes QRadar SIEM, Log Manager, Vulnerability Manager, Risk Manager, QFlow and VFLow Collectors, and Incident Forensics. QRadar can be deployed as an appliance, a virtual appliance or as SaaS/infrastructure as a service (IaaS)."
- "Components can be deployed in an all-in-one solution or scaled by using separate appliances for different functions."
- "Recent enhancements include incident forensics support, new data storage appliances, improved query support across logs, flow data, threat intelligence, and vulnerability and asset data. The capability to replay historical event data through current correlation rules is also now available."
- "IBM offers a hybrid delivery option for QRadar, with an on-premises QRadar deployment, a SaaS solution hosted on IBM Cloud and optional remote monitoring from IBM's managed security service operations centers."

And in case you had not heard…..

- *According to IDC*, IBM Security Systems:*
  - Maintained the #1 position in Identity and Access Management
  - Maintained #1 position in Security Vulnerability Management (which includes SIEM)
  - Improved its share in Endpoint Security and Network Security.
  - Significantly outpaced overall security software market growth, and remained the #3 security software vendor in 2013." *(Approved 4/23/14, IDC Permissions/Michael Shirer)*

- *Gartner published their 2014 revenue/share estimate and IBM Security Systems:*
  - 2015 Gartner rates IBM #1 in SIEM (3rd year) and #2 in Enterprise Security
  - IBM moved up to #3 in total share, and is the fastest growing security software vendor in the global market based on revenue (2014)
  - Grew +3X faster than the overall market: 19/5%

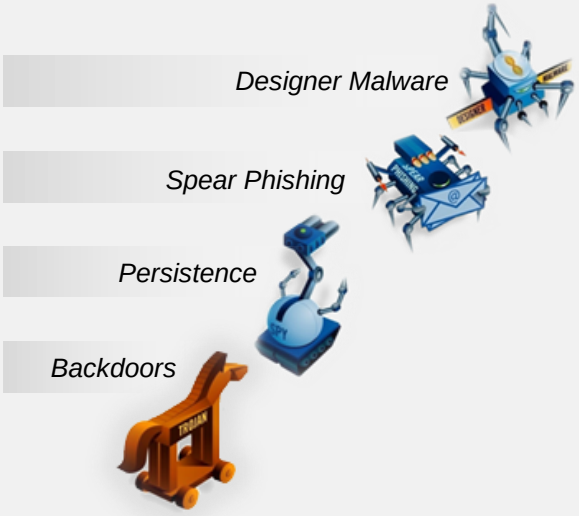
*According to IDC's Worldwide Semiannual Software Tracker analysis for calendar 2013

Agenda

- Introduction
- 2014 Gartner Magic Quadrant for SIEM
- IBM Security QRadar SIEM Solutions
  - How we got here

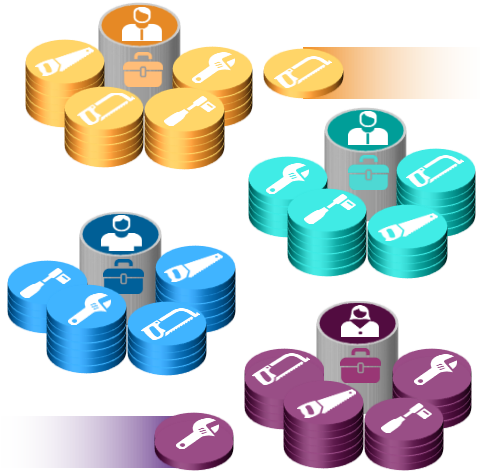
The Need for Security Intelligence – Drives Everything We Do

Escalating Threats



- Increasingly sophisticated attack methods
- Disappearing perimeters
- Accelerating security breaches

Increasing Complexity



- Constantly changing infrastructure
- Too many products from multiple vendors; costly to configure and manage
- Inadequate antivirus products

Resource Constraints

- Struggling security teams
- Too much data with limited manpower and skills to manage it all

IBM QRadar Security Intelligence Platform

Providing actionable intelligence

INTELLIGENT

Correlation, analysis and massive data reduction

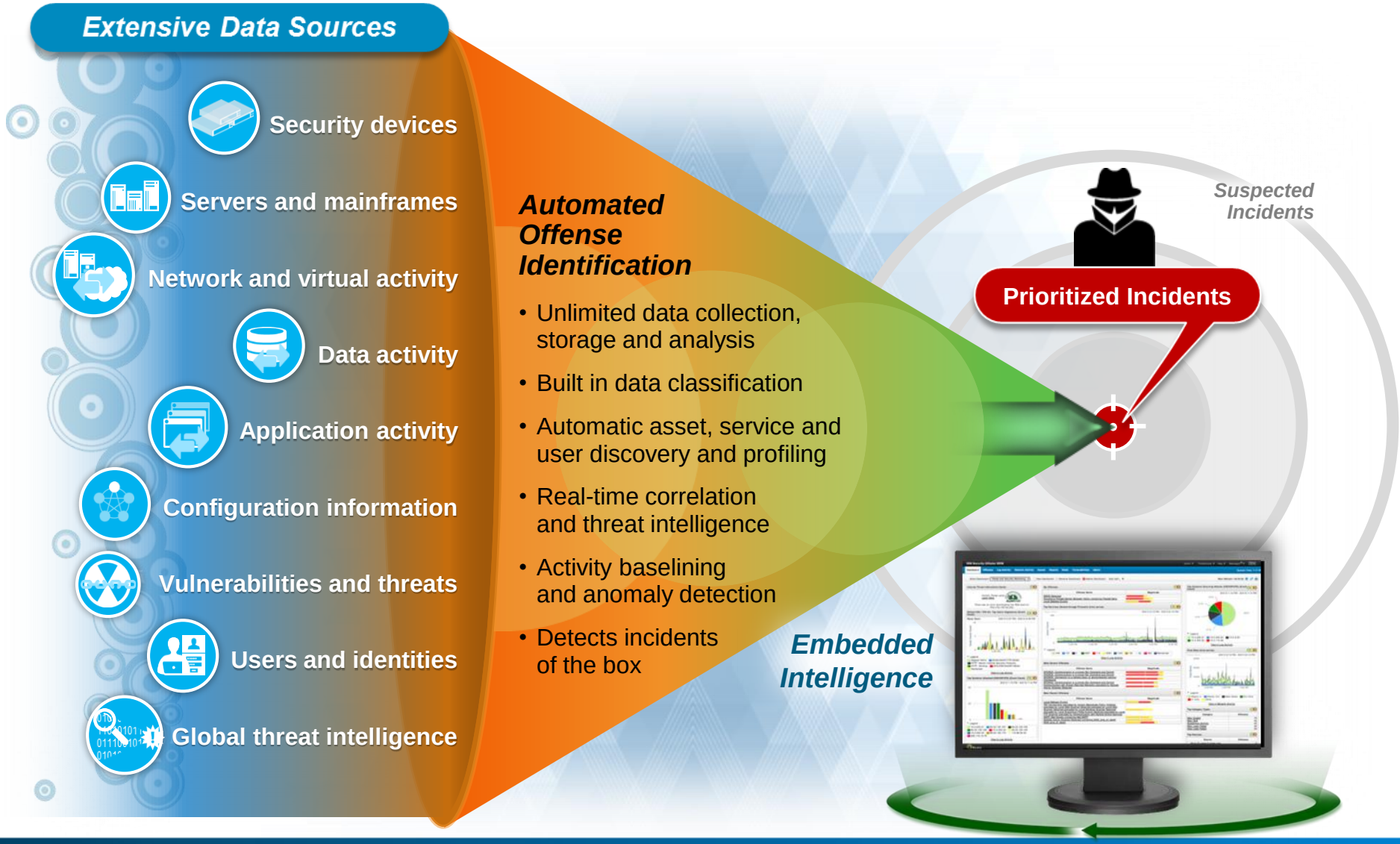
AUTOMATED

Driving simplicity and accelerating time-to-value

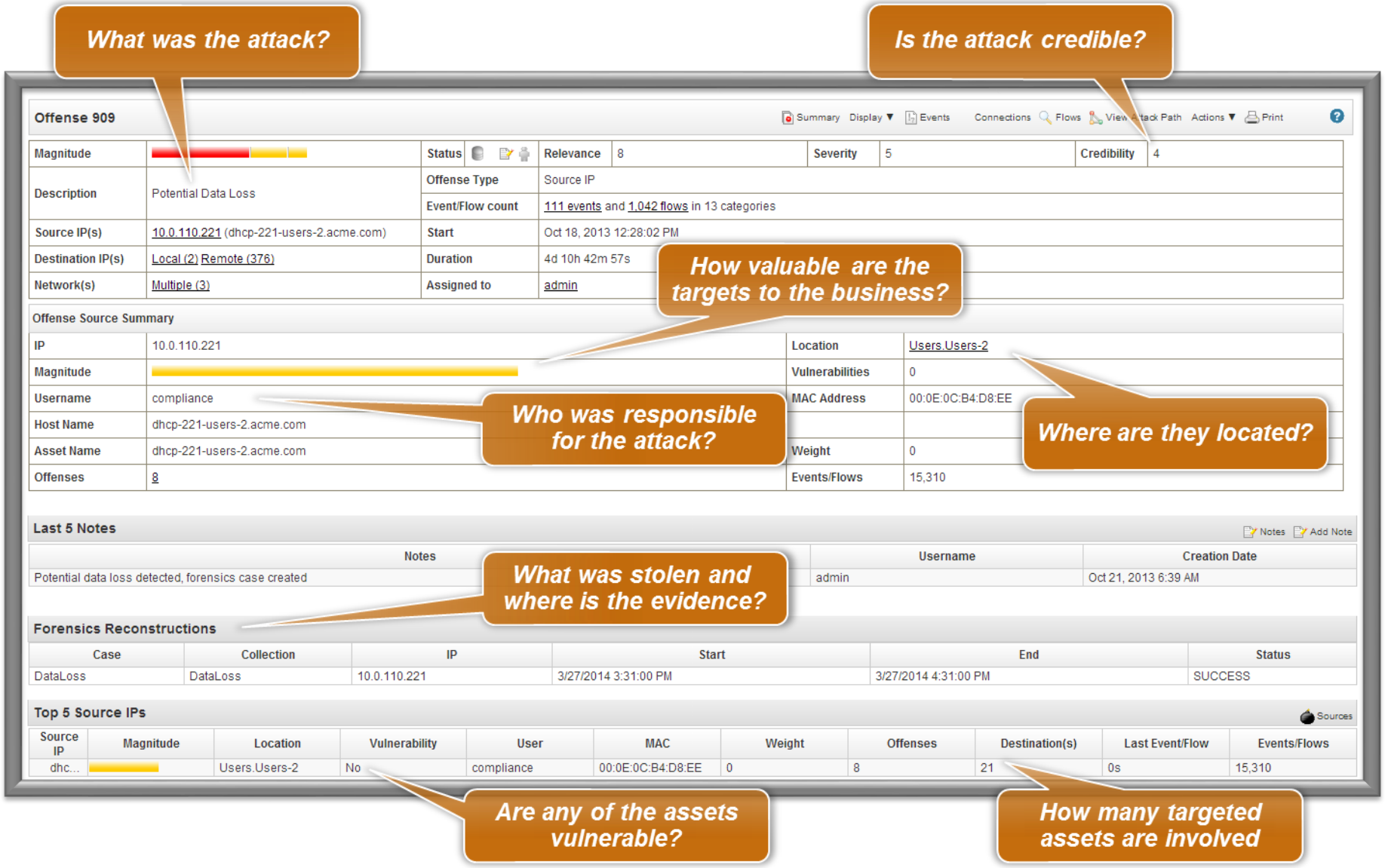
INTEGRATED

Unified architecture delivered in a single console

The Core of Our Solution: IBM Security QRadar SIEM



Answering questions to help prevent and remediate attacks



Extending the Core with In-Depth Forensics Investigation

- Security devices
- Application activity
- Servers and mainframes
- Global threat intelligence
- Network and virtual activity
- Vulnerabilities and threats
- Configuration information
- Users and identities
- Data activity

QRadar SIEM

- Automated data collection and asset discovery
- Real-time, and integrated analytics
- Massive data reduction
- Anomaly detection

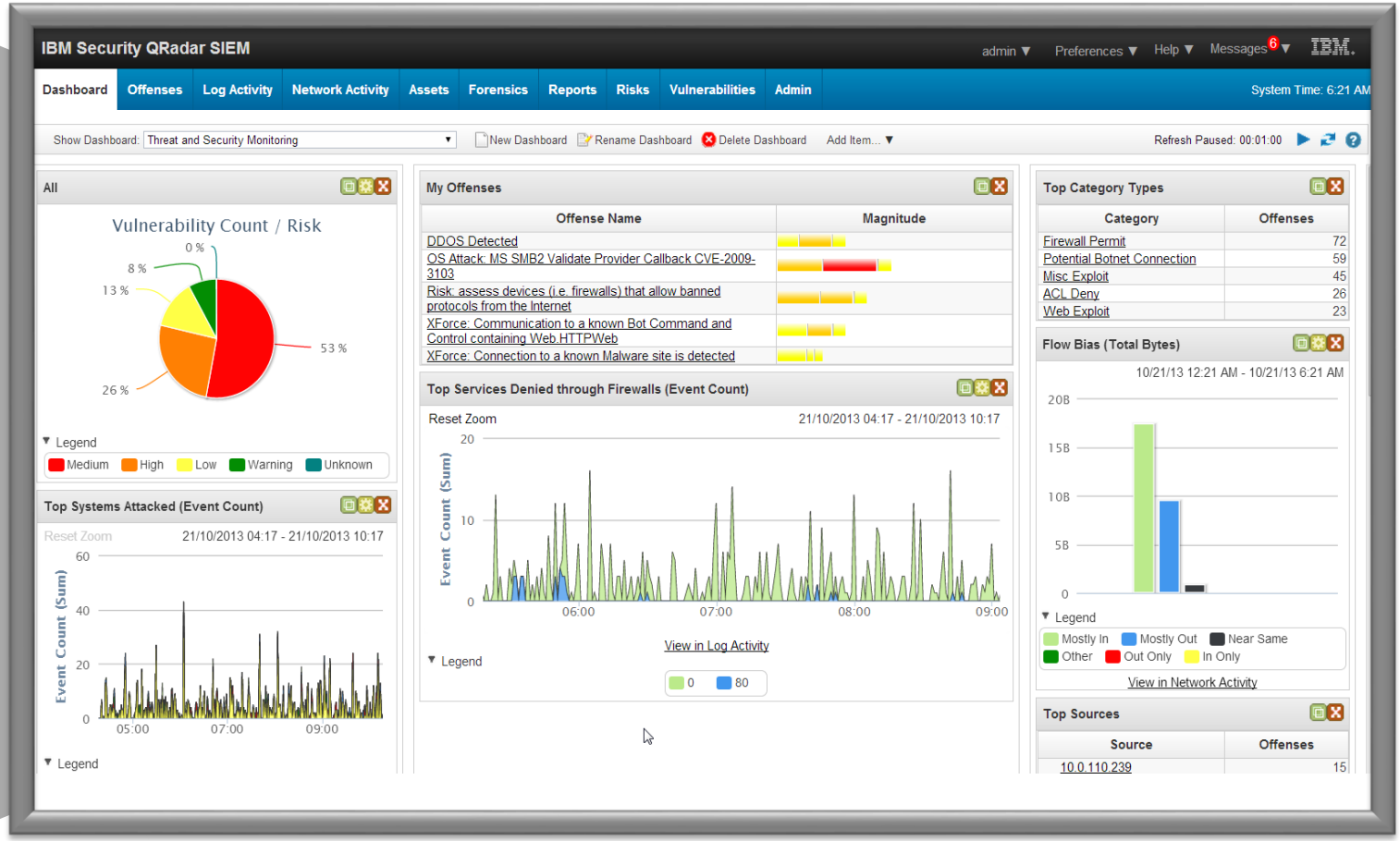
Offenses Identified by QRadar

QRadar Incident Forensics

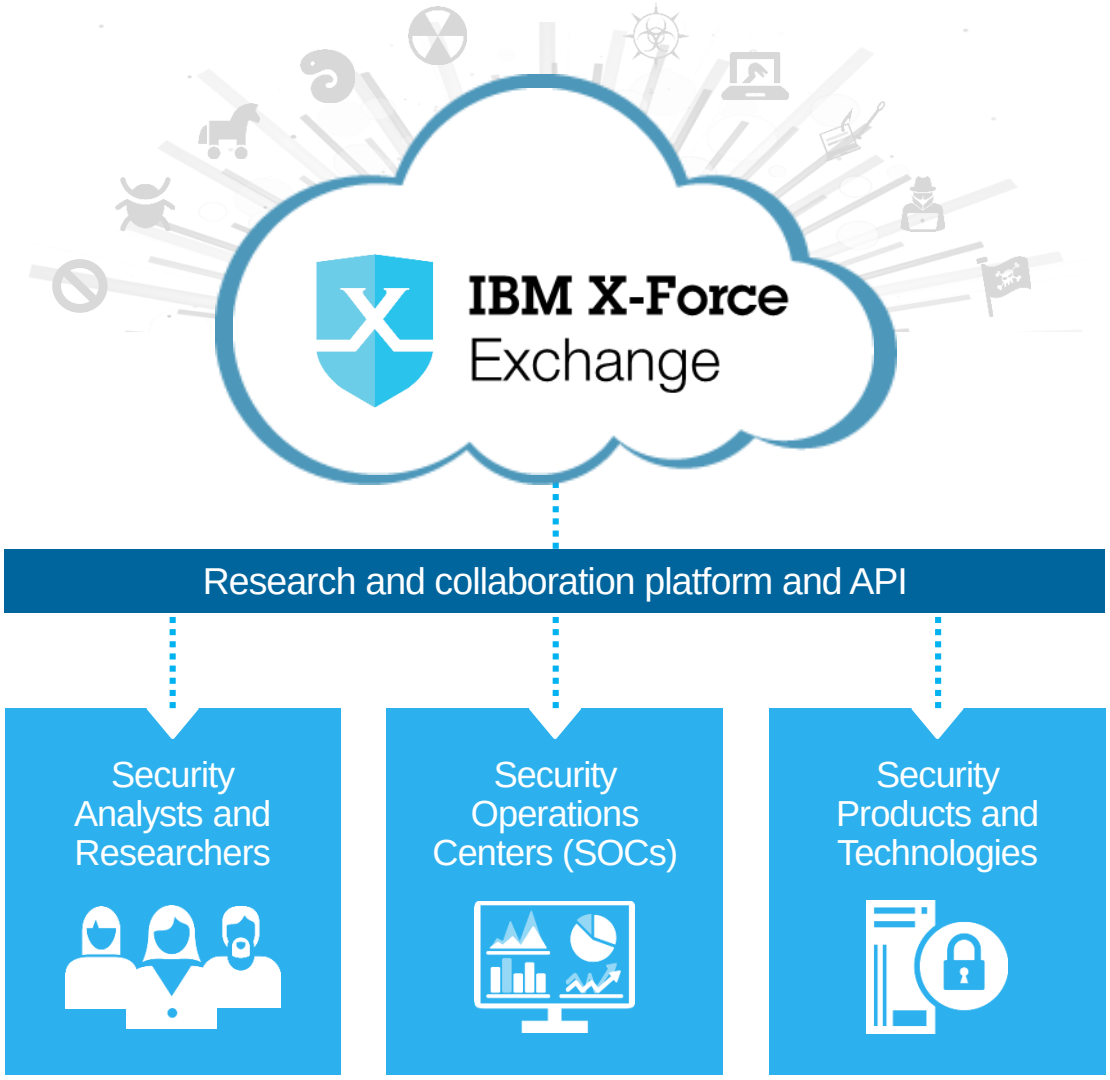
- Full PCAP Forensics
- Detailed Incident Meta-Data Evidence
- Reconstruction of content and incident activity

An integrated, unified architecture in a single web-based console

- Log Management
- Security Intelligence
- Network Activity Monitoring
- Risk Management
- Vulnerability Management
- Network Forensics



IBM X-Force Exchange Enhancing Value of QRadar



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

IBM X-Force Exchange is:

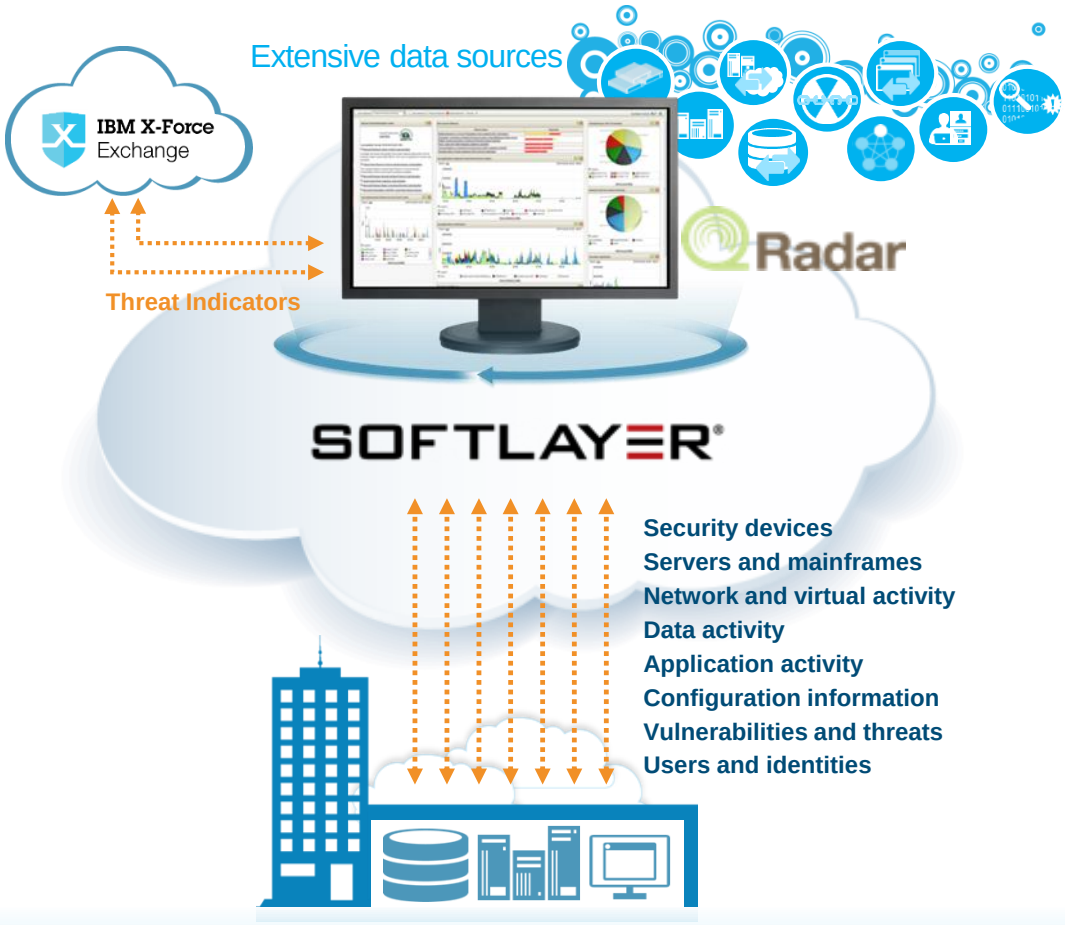
OPEN
a robust platform with access to a wealth of threat intelligence data

ACTIONABLE
an integrated solution to help quickly stop threats

SOCIAL
a collaborative platform for sharing threat intelligence

Backed by the reputation and scale of IBM X-Force

Extending QRadar Security Intelligence Platform to the Cloud



- Cloud-based offering of the #1 Security Intelligence solution
- IBM deploys, maintains and supports infrastructure
- Protects against threats and reduces compliance risk
- Leverages real-time threat intelligence from X-Force
- Collects data from both on-premise and cloud resources

Accelerate your ability to identify and stop cyber threats with

FLEXIBLE

a full suite of upgradeable security analytics offerings and service levels to choose from

COST EFFECTIVE

acquire and deploy quickly with no CapEx investment

PEACE OF MIND

trusted IBM security service professionals available to provide guidance and meet your security requirements

IBM Security QRadar for MSSPs

- Multi-tenant and single deployment options
- Master Console for centralized view of multiple clients
- System configuration template support
- Horizontal scalability
- Extensive APIs for enterprise integration
- Cloud-ready
- Flexible MSSP pricing options

New capabilities creating profitable opportunities for MSSPs

IBM QRadar is:

COST EFFECTIVE

Single and multi-tenanted enabling low cost, rapid delivery of security intelligence services

SCALABLE & FLEXIBLE

Scales as needed from the smallest to the largest customers with centralized management

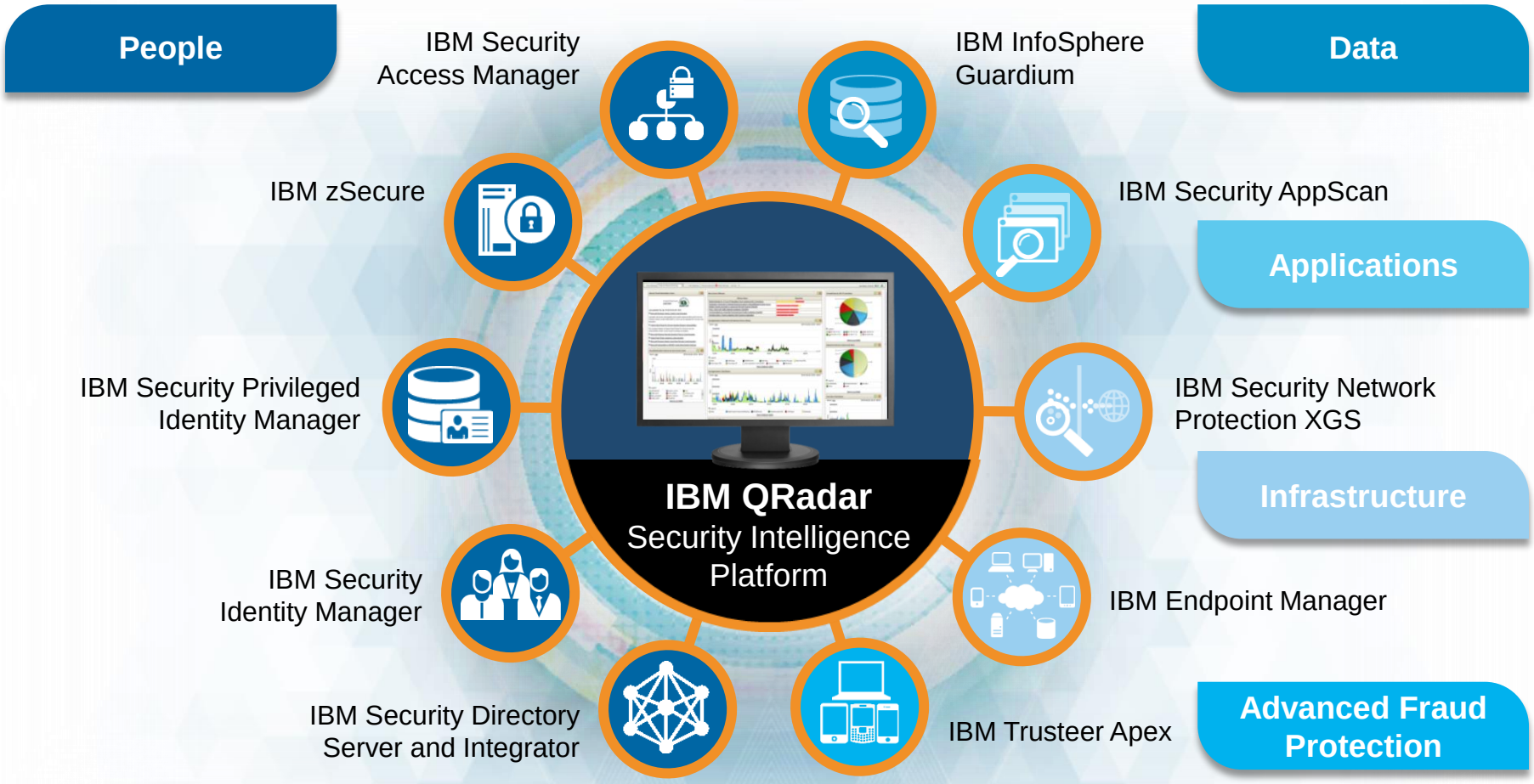
AUTOMATED

driving simplicity and accelerating time-to-value for service providers

Recent QRadar Investments and Innovations

- Advanced Search
- Historical Correlation
- X-Force Exchange Integration
- Real-Time Threat Intelligence
- Open API's for expanded integrations
- 500+ Devices, Systems and Applications Supported
- Rules/Building Blocks – over 500 enabled out-of-the-box
- Over 1600 unique reports now available

QRadar is the Centerpiece of IBM Security Integration



IBM QRadar Supports Hundreds of Third-Party Products

IBM QRadar
Security Intelligence Platform

JUNIPER NETWORKS
paloalto NETWORKS
Microsoft
IBM
symantec.
CISCO
NetApp
SAP
FireEye
McAfee
enterasys Secure Networks
SOURCEfire
vmware
Check Point SOFTWARE TECHNOLOGIES LTD.
IMPERVA
f5
BARRACUDA NETWORKS
ORACLE
BlueCoat
QUALYS
splunk>

QRadar Security Intelligence Solution Delivery Models

Capital and Operating Expense Options:

- Hardware-based appliances

- Software for qualified, client-owned servers

- Virtual appliances for VMware environments

- Cloud

Operational Expense Option:

- SaaS- Security Intelligence on Cloud

IBM Services Managed SIEM

Delivering SIEM optimization with advanced threat protection

SIEM optimization → **Managed SIEM**

Custom-tailored engagement

- SIEM design and build services
- Use case design and log acquisition
- SIEM implementation
- SIEM optimization

Steady-state SIEM management

- Threat monitoring and response
- SIEM administrative support
- SIEM infrastructure management
- SIEM reporting

More quickly identify and remediate	Consolidate data silos	Better predict business risks	Detect insider fraud	Address regulation mandates	Optimize staff resources
Deploy robust security intelligence and incident forensics	Collect, correlate and report on data in one integrated solution	Engage entire risk management lifecycle for infrastructures	Adopt next-generation SIEM with identity correlation	Automate data collection and configuration audits	Offload security monitoring and device management

IBM X-Force and Security Services – A Winning Combination

IBM Security by the Numbers

133+ monitored countries (MSS)

3300+ service delivery experts

20000+ devices under contract

270000000+ endpoints protected

15000000000+ events managed per day

Client example: An international energy company reduces billions of events per day to find those that should be investigated

Optimize threat analysis

An international energy firm analyzes

2 billion

events per day to find

20-25

potential offenses to investigate

Business challenge

- Reducing huge number of events to find the ones that need to be investigated
- Automating the process of analyzing security data

Solutions (QRadar SIEM, QFlow, Risk Manager)

Combined analysis of historical data with real-time alerts to gain a ‘big picture’ view and uncover patterns of unusual activity humans miss and immediately block suspected traffic

Learn more about IBM Security QRadar SIEM

Download the 2015 Gartner Magic Quadrant for SIEM

Read our blog

Visit our Website:
http://ibm.co/QRadar

Learn more about IBM Security

IBM Security

TOP 3 enterprise security software vendor in total revenue

20 industry analyst reports rank IBM Security as a **LEADER**

133 countries where IBM delivers managed security services

10K clients protected *including…*

24 of the top 33 banks in Japan, North America, and Australia

Visit our web page
IBM.com/Security

Watch our videos
IBM Security YouTube Channel

Read new blog posts
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

IBM Security

Intelligence. Integration. Expertise.

IBM

Q&A

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.

THANK YOU

www.ibm.com/security

IBM **Security**

Intelligence. Integration. Expertise.