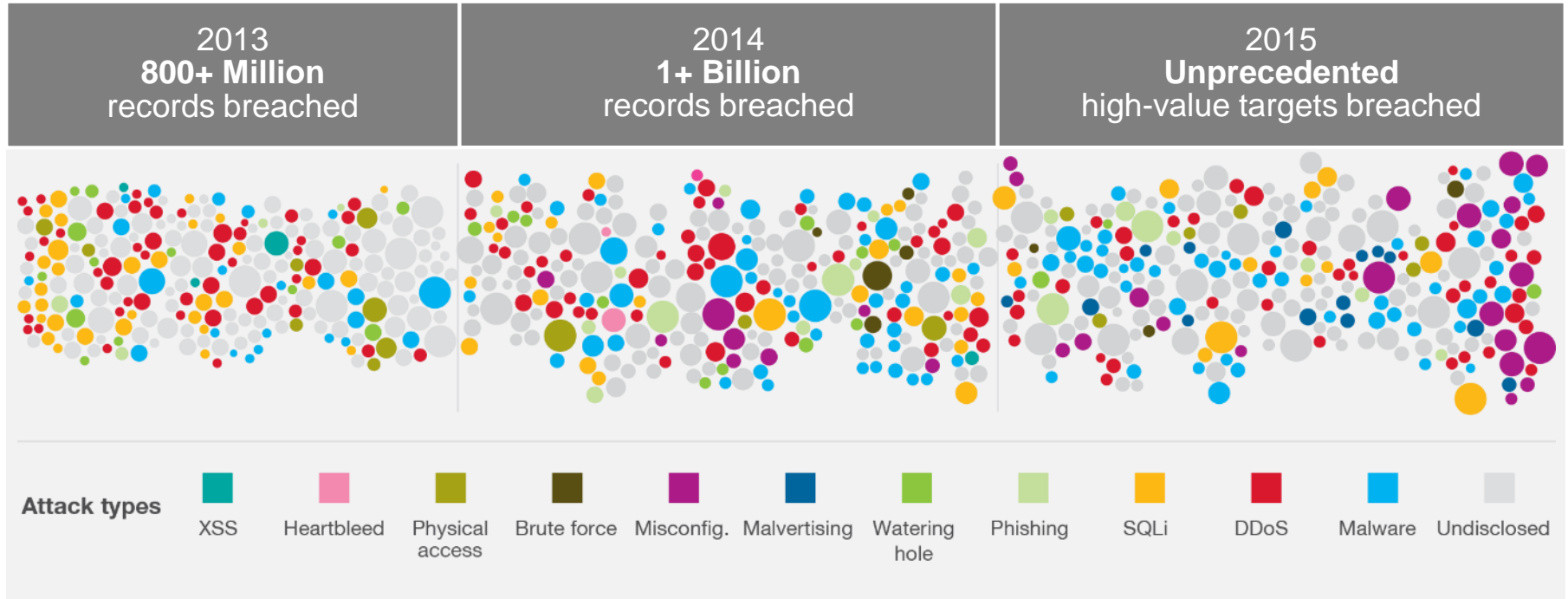


The Power of Security Analytics

Anticipate the unknown. Sense it and act.



Attackers break through conventional safeguards every day



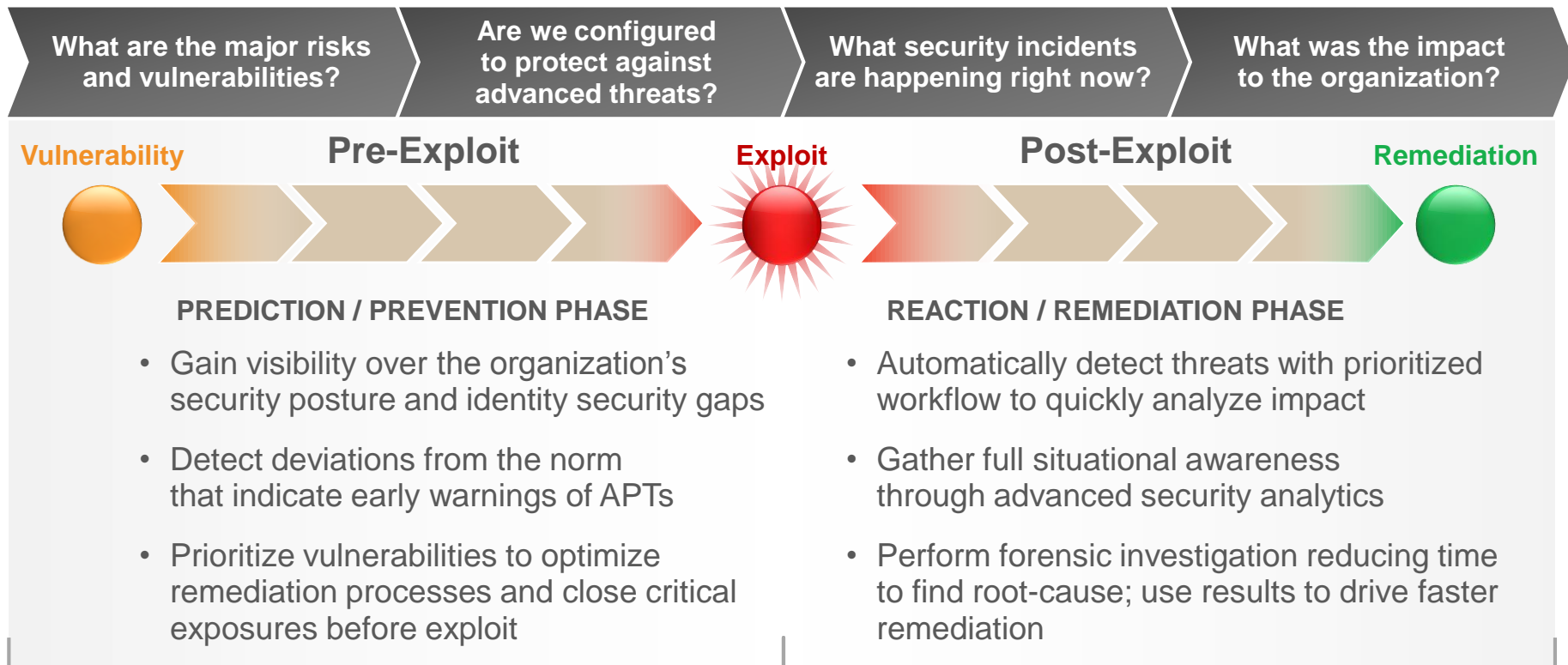
average time to detect APTs

256 days

average cost of a U.S. data breach

\$6.5M

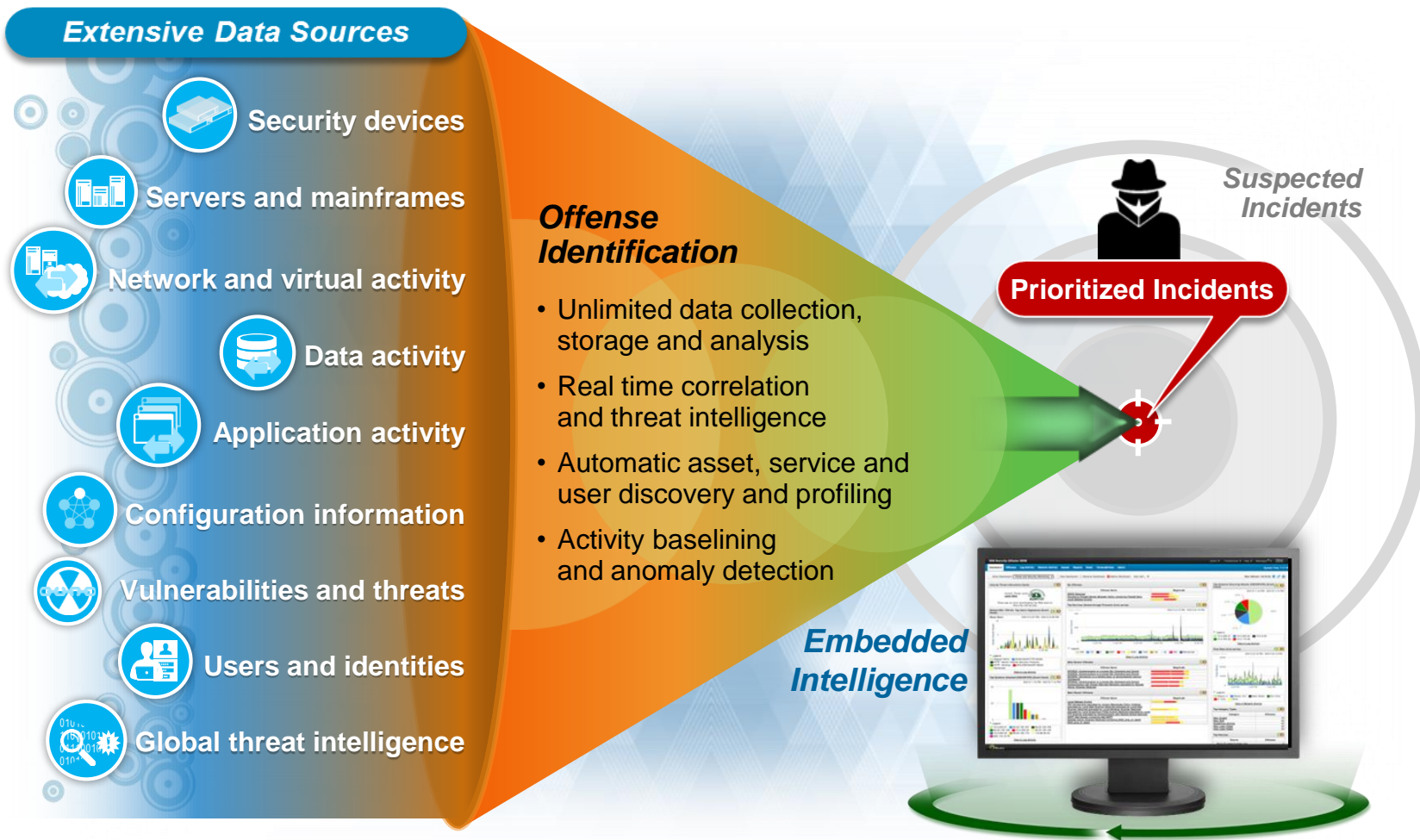
Develop a strategy and ask the right questions



Security Intelligence

The actionable information derived from the analysis of security-relevant data available to an organization

Consume massive amount of structured and unstructured data



IBM Security QRadar – Success Factors

Sense Analytics™ Threat Detection



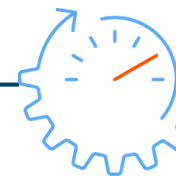
Behavioral
Contextual
Temporal

One Platform, Unified Visibility



Extensible
Scalable
Easily deployed

The Power to Act—at Scale



Prioritization
**Collaboration of
threat data**
**Automated
response**

QRadar Sense Analytics™

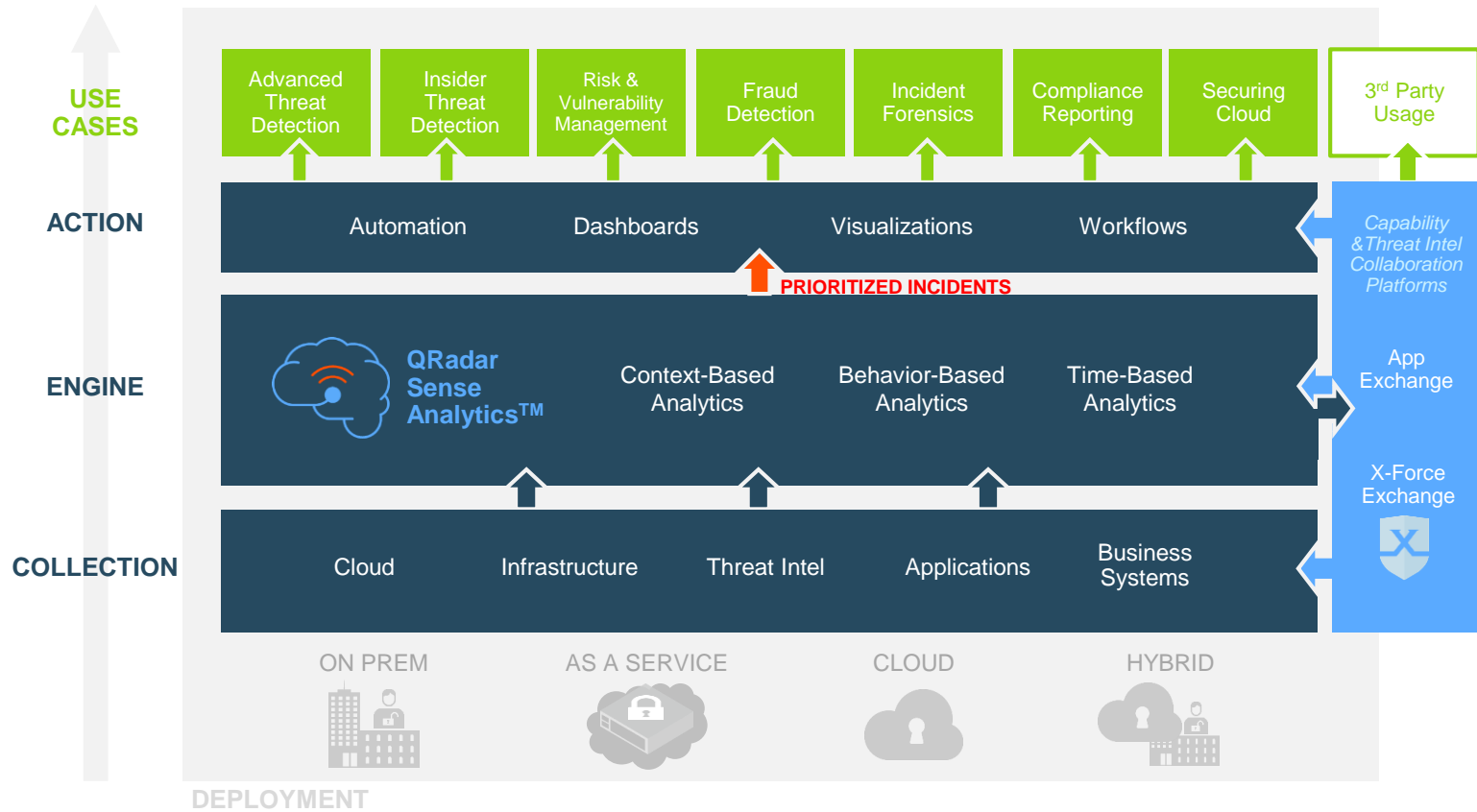


**Advanced analytics
assisting in threat
identification**

QRadar is the only Security Intelligence Platform powered by the advanced **Sense Analytics** engine to:

- *Detect abnormal behaviors across users, networks, applications and data*
- *Discover current and historical connections, bringing hidden indicators of attack to the surface*
- *Find and prioritize weaknesses before they're exploited*

QRadar Sense Platform

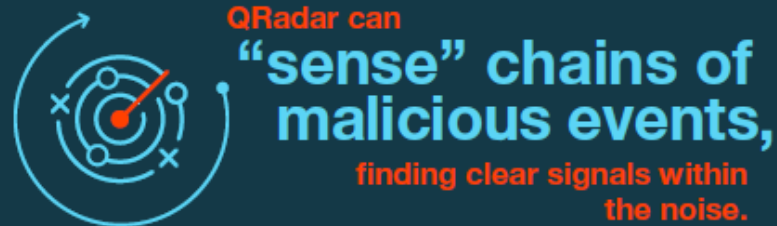


Advanced threat detection

Situational Assessment:

Malicious domain

- System sees new beaconing activity and data transfers inconsistent with behavioral baselines appear
- QRadar combines multiple conditions to produce single, heightened alert



**Pattern
Identification**

**Anomaly
Detection**

**User & Entity
Profiling**

Insider threat monitoring

Situational Assessment:

Terminated employee

- Service rep downloads 2X normal amount of client data
- But QRadar knows that representative was recently laid off and sees data being sent to an external site.

**Business
Context**

**Historical
analytics**

**Risk-based
Analytics**



Many of the world's largest
companies rely on QRadar to help

**keep them
out of the news.**

Forensics investigation

Situational Assessment:

Terminated employee

- SOC analyst investigating offense discovers employees exposed to phishing scam
- Attacker has latched-on and expanded to an internal server using pattern identified by X-Force known to inject remote-access Trojan (RAT) software.

**Real time
analytics**

**External Threat
Correlation**

**Statistical
Analysis**



QRadar takes

**the mystery
out of security
investigations,**

**helping security teams identify attackers, their
tactics and where the initial breach occurred.**

One platform with global visibility

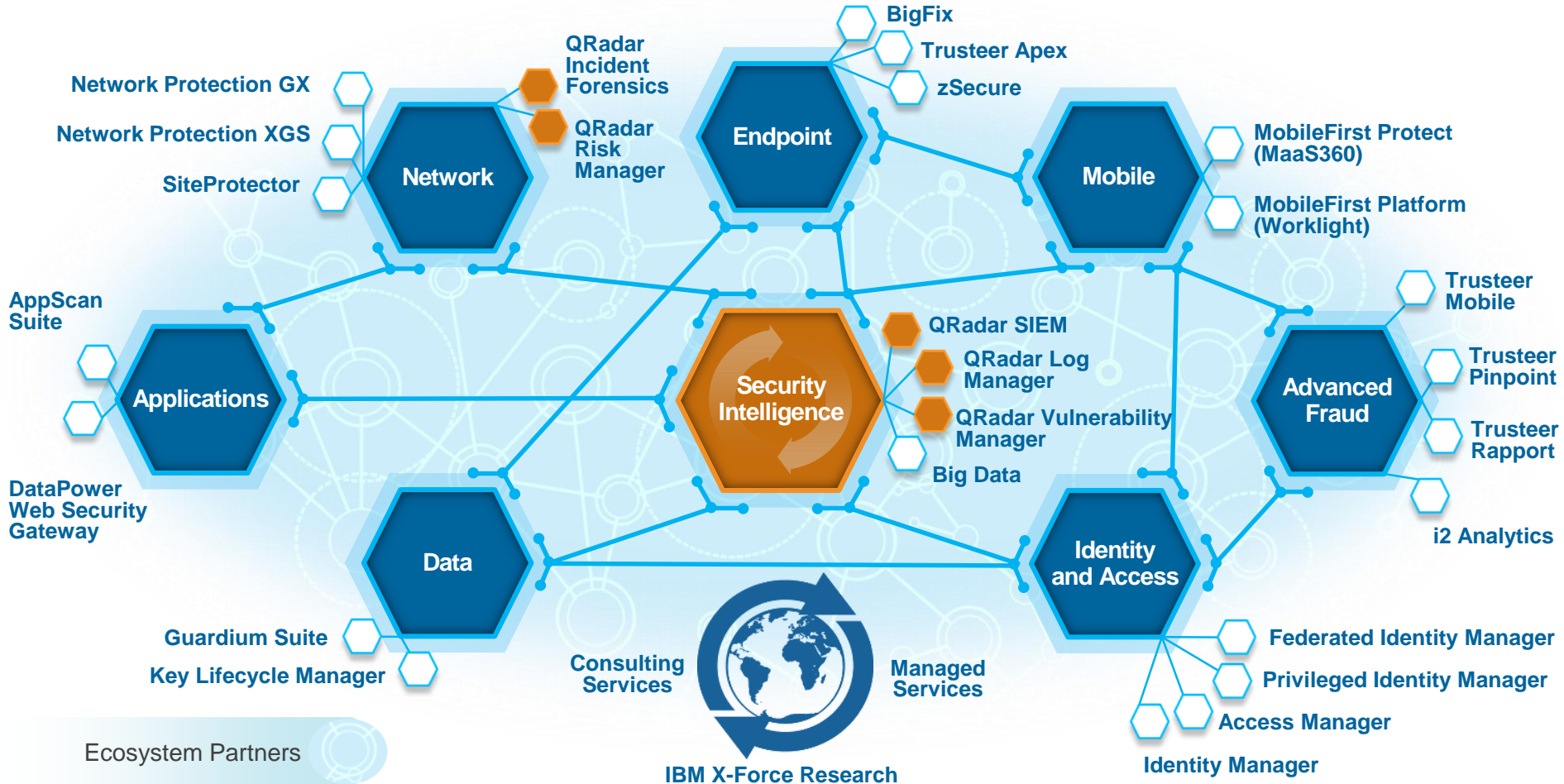


**Complete clarity
and context**

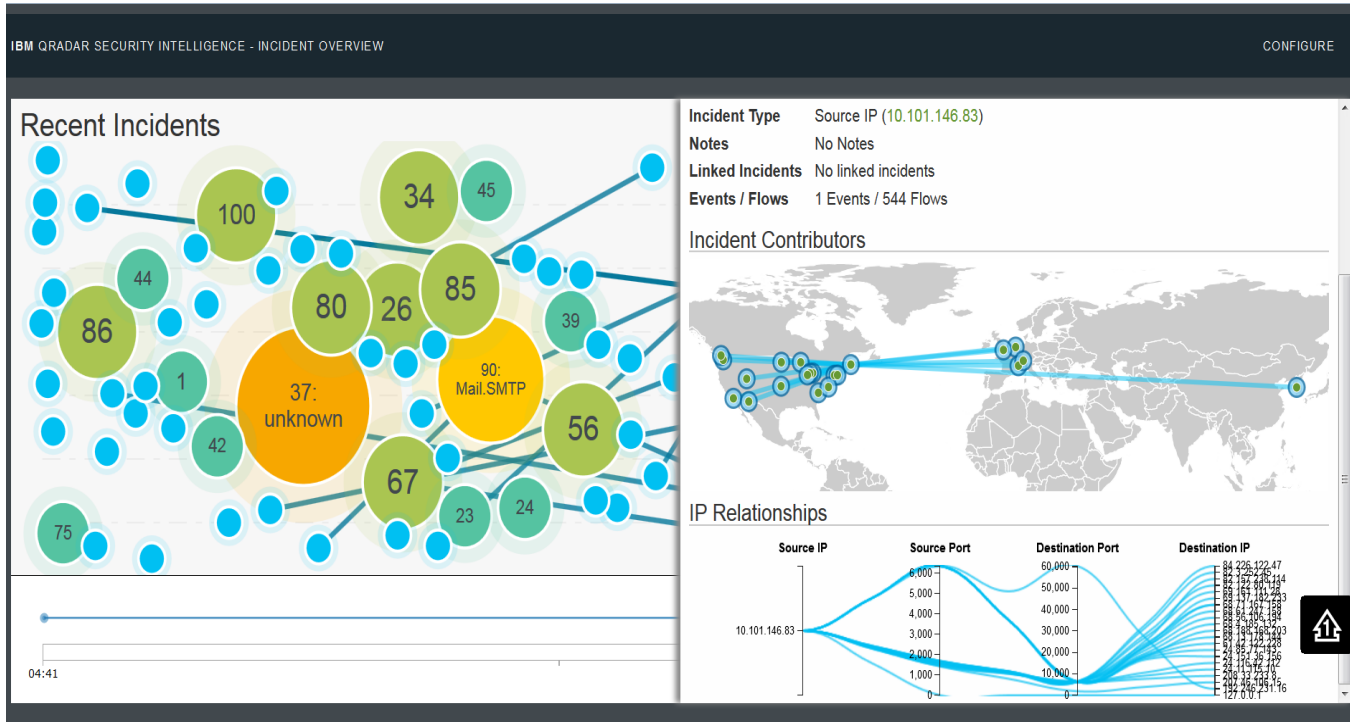
QRadar easily deploys lightning fast to help users consolidate insights in a single platform:

- *Delivers scale collecting billions of events on-premises or in the cloud*
- *Unifies real-time monitoring, vulnerability and risk management, and forensics*
- *Deep and automated integration from hundreds of 3rd party sources*

Aggregate and interpret all your security data



Visualize your threat landscape

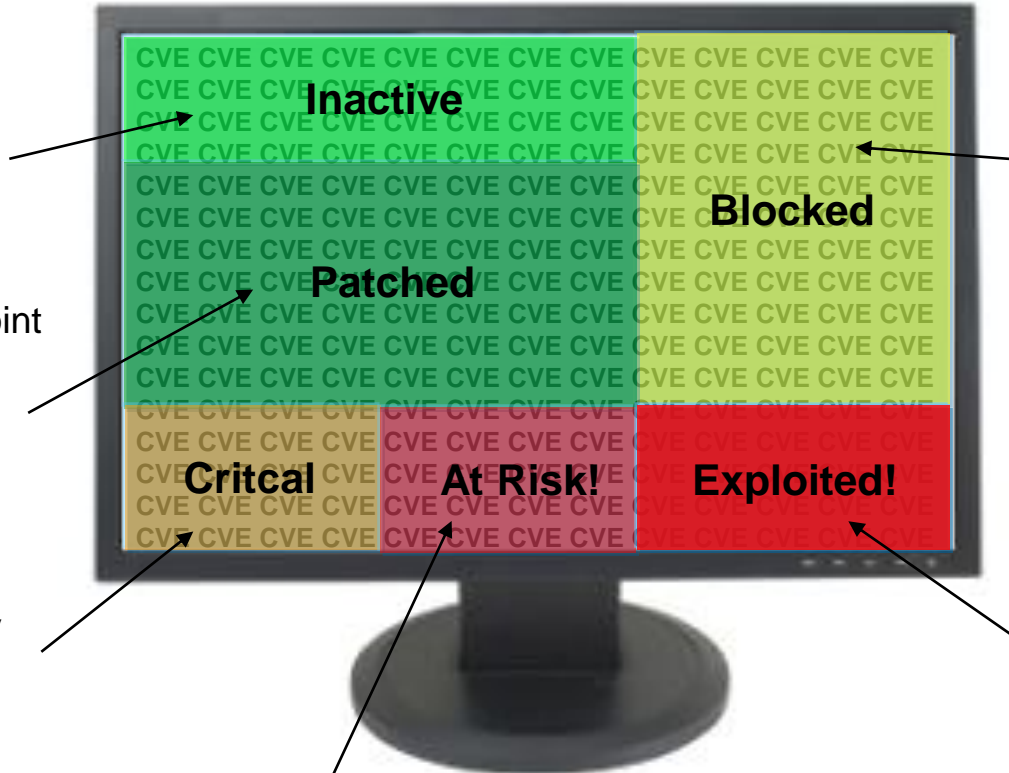


Prioritize your vulnerabilities

Inactive: QFlow Collector data helps QRadar Vulnerability Manager sense application activity

Patched: IBM Endpoint Manager helps QVM understand which vulnerabilities will be patched

Critical: Vulnerability knowledge base, remediation flow and QRM policies inform QVM about business critical vulnerabilities



Blocked: QRadar Risk Manager helps QVM understand which vulnerabilities are blocked by firewalls and IPSs

Exploited: SIEM correlation and IPS data help QVM reveal which vulnerabilities have been exploited

At Risk: X-Force Threat and SIEM security incident data help QVM see assets communicating with potential threats

The power to act at scale

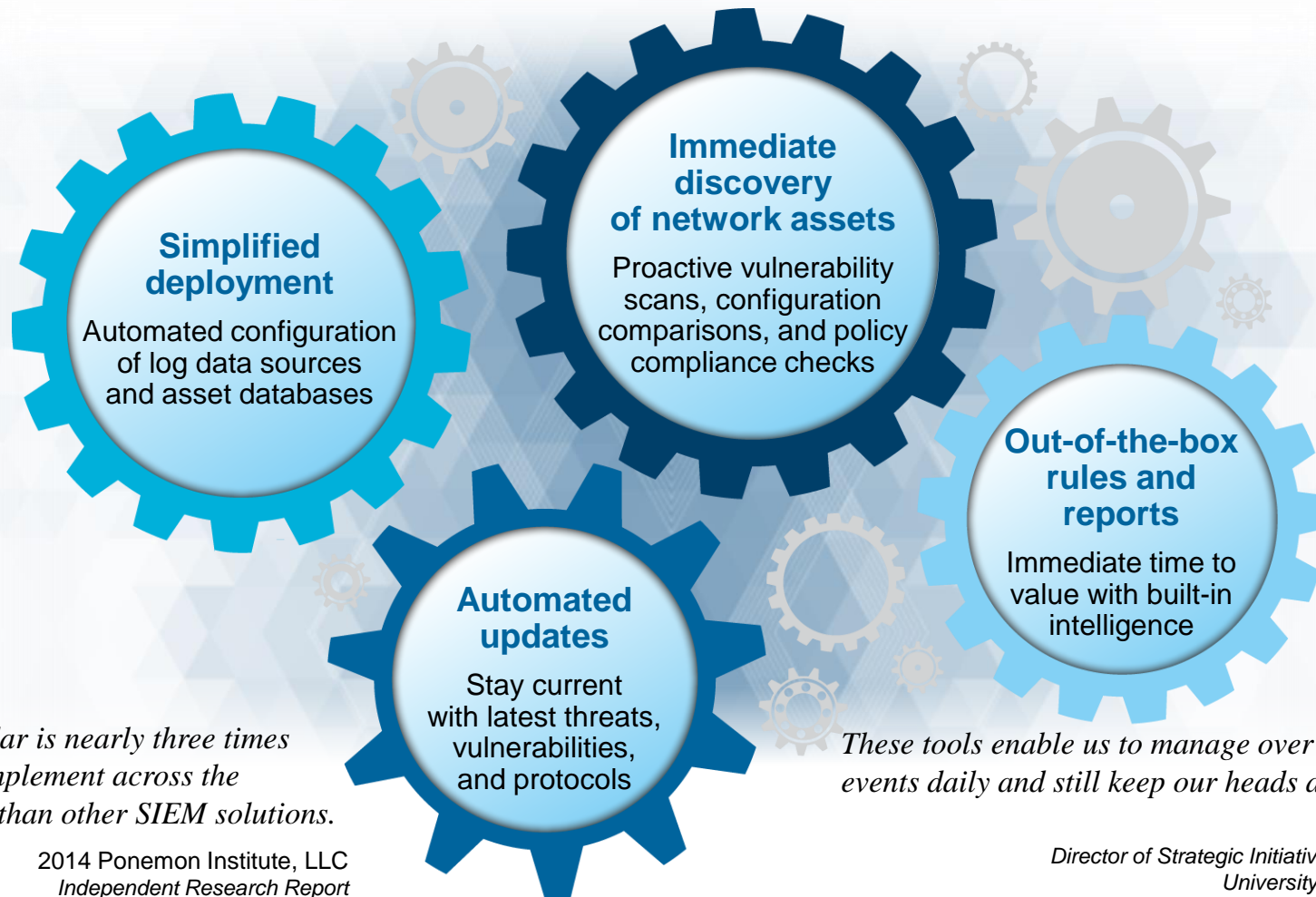


**Actionable
security
intelligence**

QRadar enables security experts within and across organizations to **collaboratively take action:**

- *Intelligent incident prioritization*
- *Collaboration of threat data and security capabilities from X-Force Exchange and App Exchange*
- *Resilient incident response with automation and workflows*

Realize value in days



IBM QRadar is nearly three times faster to implement across the enterprise than other SIEM solutions.

2014 Ponemon Institute, LLC
Independent Research Report

These tools enable us to manage over 2.2 million events daily and still keep our heads above water.

David Shipley
Director of Strategic Initiatives and IT Services
University of New Brunswick

Achieve focus with forensics investigations

The image displays the IBM QRadar Security Intelligence interface, illustrating forensic investigation capabilities. The main window shows a search for "Content: Secret" across 82,114 documents. The interface includes a navigation bar with tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Forensics, Reports, Risks, Vulnerabilities, and Admin. The system time is 6:11 AM.

Key features highlighted in the interface include:

- Search Bar:** Contains the search query "Content: Secret".
- Search Results:** A table with columns: Row, Sel, Rel, Time Stamp, Application Protocol, Description, and Content. The first row shows a document from 2014/02/07 03:02:29 PM, IRC, IRC Chat Message.
- Actions:** Buttons for "Surveyor", "Digital Impression", "Export", and "Visualize".
- Grid View:** A table with columns: Id, Date, Protocol, Description, and Relevancy (1). It lists 41 search results, including web pages and email attachments.
- Network Visualization:** A graph showing relationships between IP addresses and email addresses. Nodes include IP addresses like 192.168.2.29 and 212.169.77.29, and email addresses like cresspo.edhues@cs.columbia.edu and warisfargoo@shawmutecollege.com.

Row	Sel	Rel	Time Stamp	Application Protocol	Description	Content
1			2014/02/07 03:02:29 PM	IRC	IRC Chat Message	...choopa.nj.us.dal.net 322 ...ay #Kema...

Id	Date	Protocol	Description	Relevancy (1)
23	2014/02/07 02:28:23 PM	HTTP	Web Page	1
24	2014/02/07 02:30:09 PM	HTTP	Web Page	1
25	2014/02/07 02:30:27 PM	HTTP	Web Page	1
26	2014/02/07 02:31:25 PM	HTTP	Web Page	1
27	2014/02/07 02:31:52 PM	HTTP	Web Page	1
28	2014/02/07 02:32:20 PM	HTTP	Web Page	1
29	2014/02/07 02:34:08 PM	HTTP	Web Page	1
30	2014/02/07 02:34:11 PM	HTTP	Email Attachment	1
31	2014/02/07 02:35:34 PM	HTTP	Web Page	1
32	2014/02/07 02:36:46 PM	HTTP	Web Page	1
33	2014/02/07 02:36:58 PM	HTTP	Web Page	1
34	2014/02/07 02:40:57 PM	HTTP	Web Page	1
35	2014/02/07 02:46:11 PM	HTTP	Web Page	1
36	2014/02/07 02:47:49 PM	HTTP	Web Page	1
37	2014/02/07 02:47:52 PM	HTTP	Web Page	1
38	2014/02/07 02:48:19 PM	HTTP	Web Page	1
39	2014/02/07 02:48:48 PM	HTTP	Web Page	1
40	2014/02/07 02:51:02 PM	HTTP	Web Page	1
41	2014/02/07 02:51:19 PM	HTTP	Web Page	1
42	2014/02/07 02:51:55 PM	HTTP	Web Page	1
43	2014/02/07 02:52:01 PM	HTTP	Web Page	1

Leverage multiple threat intelligence sources



Current Threat Activity

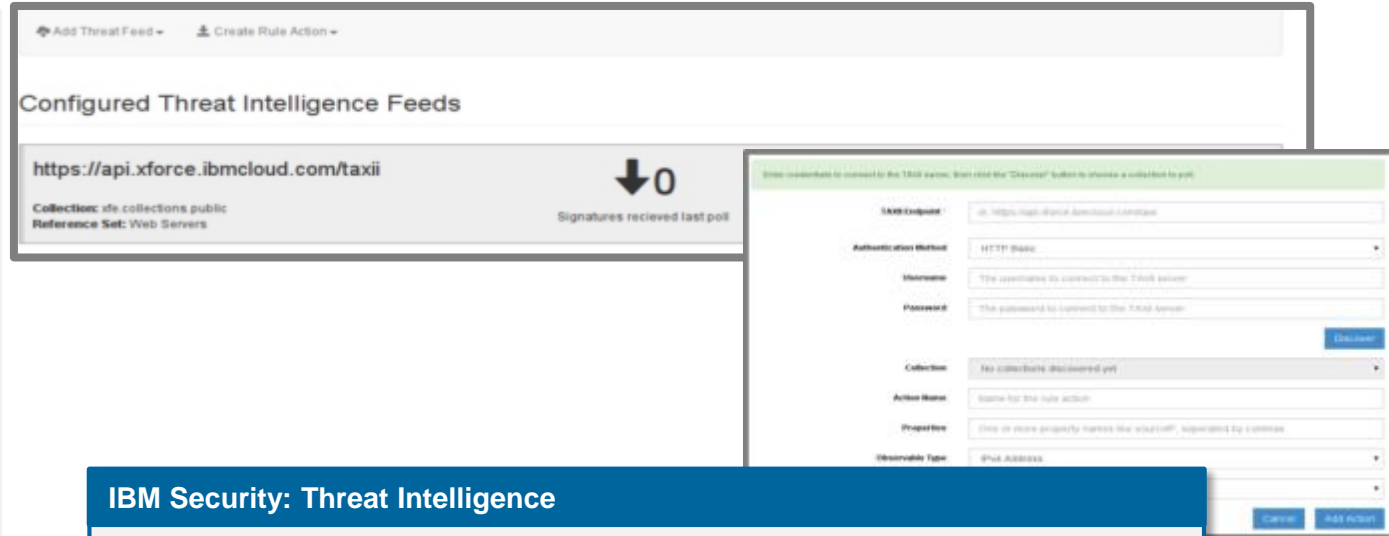
787

IBM Security
Identity and Access Management

ALERTCON

STIX™

TAXII™



Configured Threat Intelligence Feeds

<https://api.xforce.ibmcloud.com/taxii>

Collection: xfc_collections_public
Reference Set: Web Servers

Signatures received last poll: 0

IBM Security: Threat Intelligence

IBM Security: Threat Intelligence configuration form:

- URL Endpoint:
- Authentication Method: HTTP Basic
- Username:
- Password:
- Collection:
- Action Name:
- Properties:
- Observable Type:

IBM Security: Threat Intelligence

- Pull in Threat Intelligence through open STIX/TAXII format
- Load threat indicators in collections into QRadar Reference sets
- Use reference sets for correlation, searching, reporting
- Create custom rule response to post IOCs to Collection
- USE CASE:
Bring watchlists of IP addresses from X-Force Exchange create a rule to raise the magnitude of any offense that includes the IP watchlist

Add collaborative defenses – App Exchange



Validated
Security Apps

Single Platform
for Collaboration

Access
Partner Innovations

Quickly Extend
QRadar Functionality

A New Platform for Security Intelligence Collaboration

Search by Application Create IBM ID Log In

Welcome to the Security App Exchange

Find. Download. Use.
Verified extensions for a stronger enterprise defense.

Featured

- BrightPoint Security Sentinel**
BrightPoint Security Inc
BPS Sentinel Analytics Tab shows details for an IOC
★★★★★
- Carbon Black App for IBM QRadar**
Bit9 + Carbon Black
Access process searches, endpoint isolation and system status from Carbo ...
★★★★★
- Exabeam User Behavior Analytics**
Exabeam
Exabeam is a user behavior analytics solution that leverages existing lo ...
★★★★★
- Resilient Systems Integration for QRadar**
Resilient Systems, Inc.
Integrate the Resilient Incident Response Platform (IRP) with IBM QRadar ...
★★★★★

All Applications (27) Sort By **Newest**

Single collaboration platform for rapidly delivering
new apps and content for IBM Security solutions

Allows QRadar users and partners to
deploy new use cases in an accelerated way

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.

© Copyright IBM Corporation 2015. 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. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. 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.

Legal notices and disclaimers

Copyright © 2015 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

U.S. Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.

Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS document is distributed "AS IS" without any warranty, either express or implied. In no event shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.

IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice. Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

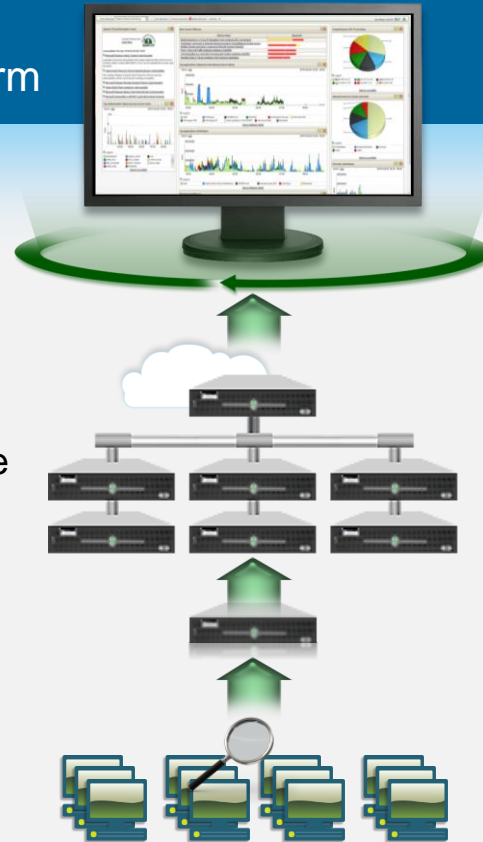
Other company, product, or service names may be trademarks or service marks of others. A current list of IBM trademarks is available at "Copyright and trademark information" www.ibm.com/legal/copytrade.shtml

Optimized appliance and software architecture for high performance and rapid deployment

IBM QRadar Security Intelligence Platform

Scalable appliance architecture








- Easy-to-deploy, scalable model using stackable distributed appliances
- Does not require third-party databases or storage



Shared modular infrastructure

- Offers automatic failover and disaster recovery
- Virtual deployments well suited for cloud environments

Reduce costs, increase visibility with an integrated platform

 Traditional SIEM <i>6 products from 6 vendors</i>			
<i>Flows</i>			 Think fast.™
<i>Packets</i>			
<i>Vulnerabilities</i>			
<i>Configurations</i>			 
<i>Logs</i>			
<i>Events</i>			

IBM Security Intelligence and Analytics



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



**IBM Security QRadar
Security Intelligence Platform**

Got data? Need analytics



Show me the threat(s) I need to deal with



Prioritize the threats for action



Take immediate action