



# 智胜威胁， 进入感知分析新纪元

IBM安全免疫系统虚拟网络峰会





智胜威胁，  
进入感知分析新纪元

IBM安全免疫系统虚拟网络峰会

# IBM安全免疫系统，助力企业发展

吴异刚

IBM客户安全专家

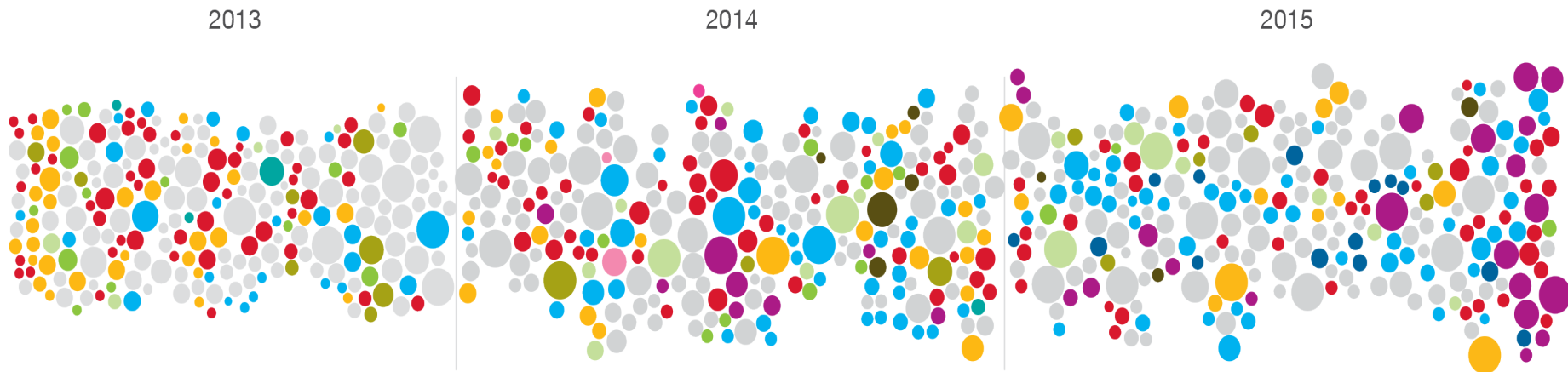


# 安全事件历史回顾（按攻击类型、时间和影响划分）

---来自IBM x-force 报告

## Sampling of security incidents by attack type, time and impact, 2013 through 2015

Size of circle estimates relative impact of incident in terms of cost to business, based on publicly disclosed information regarding leaked records and financial losses.



Attack types



XSS



Heartbleed



Physical access



Brute force



Misconfig.



Malvertising



Watering hole



Phishing



SQLi



DDoS



Malware



Undisclosed

# 256 days

APT's 平均检测时间

# \$6.5M

一次泄露的平均损失(美国)

来源: IBM X-Force® 研究和开发

# 建设安全免疫系统

网络可见性

漏洞评估

设备管理

日志，流和数据分析

防病毒

防欺诈保护

异常检测

事件和威胁管理

交易保护

防火墙

特权帐户管理

应用扫描

权利和角色

访问控制

刑事检测

恶意软件防护

数据监控

沙箱

应用安全管理

内容安全

虚拟补丁

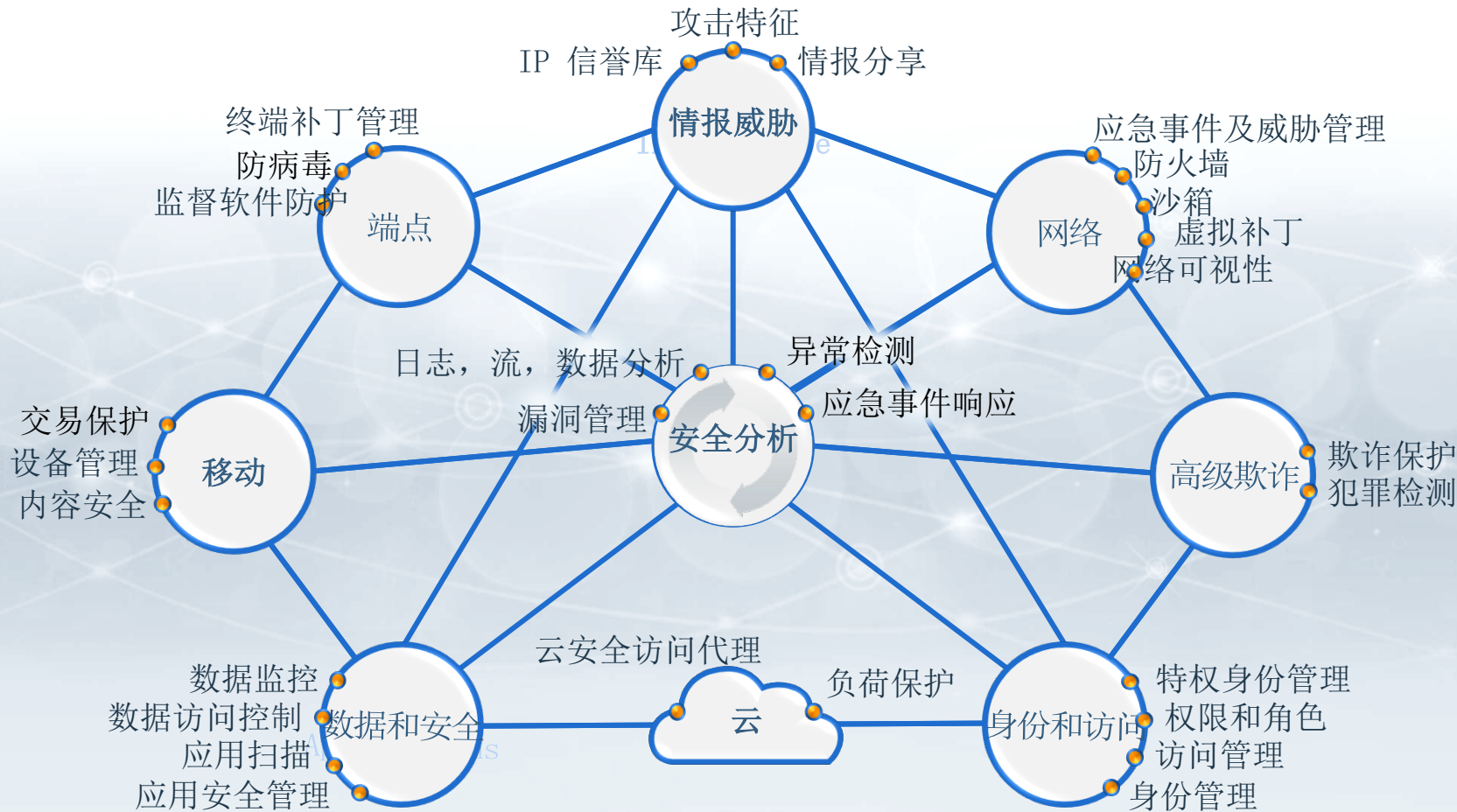
端点补丁和管理

身份管理

数据访问控制

应急事件响应

# 一种集成的智能安全免疫系统



# IBM 拥有世界最广度和深度安全体系

App Exchange  
协作应用商店

BigFix 端点

X-Force Exchange 威胁情报

Network Protection XGS 网络入侵防护

QRadar Incident Forensics 事件取证

## SECURITY OPERATIONS AND RESPONSE 安全运营和响应

QRadar SIEM安全威胁情报平台

QRadar Risk Manager 风险管理

QRadar Vulnerability Manager漏洞管理

Resilient Incident Response 应急事件响应

MaaS360移动

Trusteer Pinpoint 间谍软件检测

Trusteer Mobile 移动SDK

Trusteer Rapport 恶意软件 钓鱼检测

## INFORMATION RISK AND PROTECTION 信息风险和保护

Guardium数据

Key Manager密钥管理

AppScan应用

Identity Governance and Access 身份治理和访问

Privileged Identity Manager 特权身份管理

Cloud Identity Service 云身份服务

zSecure 大型机安全

Cloud Security Enforcer 云安全代理

## SECURITY TRANSFORMATION SERVICES 安全转型服务

管理咨询 | 系统集成 | 安全管理

# IBM Security Product Portfolio

## IBM 安全产品家族一览表

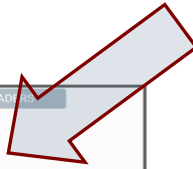
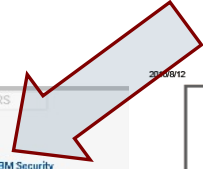
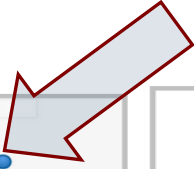
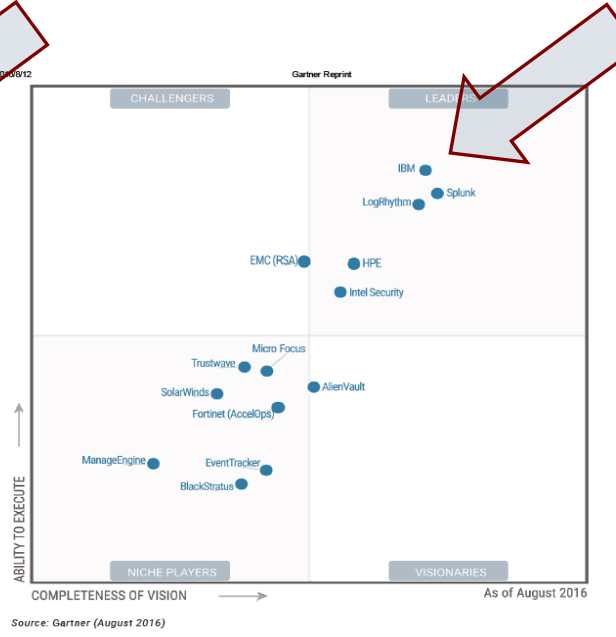
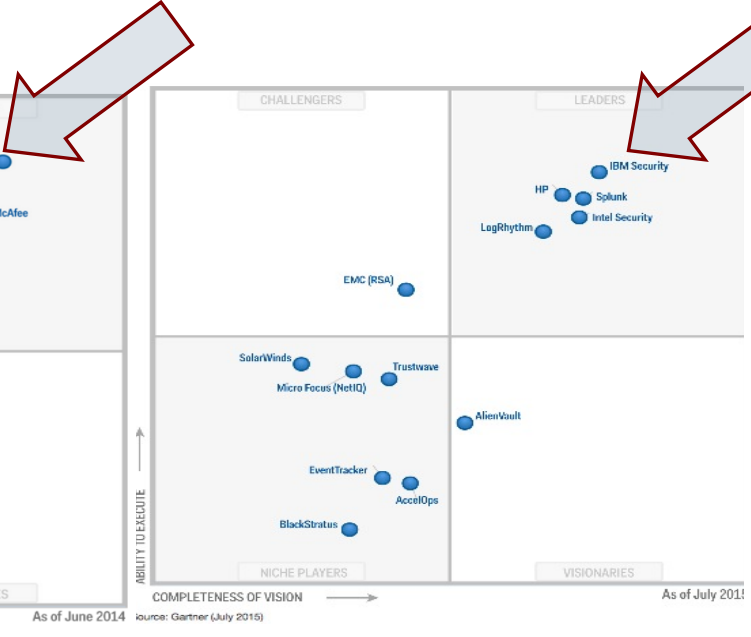
### Security Intelligence and Analytics 安全情报威胁与分析

QRadar Log Manager	QRadar Security Intelligence	QRadar Risk Manager	QRadar Vulnerability Manager	QRadar Incident Forensics
高级威胁防护	身份与权限管理	数据安全	应用安全	终端安全防护
Trusteer Rapport	Identity Governance	Guardium Data Activity Monitoring	AppScan Source	Next Generation Network Protection (XGS)
Trusteer Pinpoint Malware Detection	Identity Manager		AppScan Standard	SiteProtector Threat Management
	Trusteer Pinpoint Criminal Detection	Privileged Identity Manager	AppScan Enterprise	Trusteer Apex
Access Manager for Web Access Manager for Mobile		Guardium Data Encryption		IBM BigFix
Trusteer Mobile	Federated Identity Manager	Optim Data Privacy	DataPower Web Security Gateway	IBM MaaS360 (FiberLink)
	Directory Integrator / Directory Server	Key Lifecycle Manager	Security Policy Manager	IBM Cloud Security Enforcer
				zSecure

### IBM X-Force Research 安全实验室

2016-01-11

# SIEM象限领导位置





# 将各种情报整合起来自动发现各种攻击

## Extensive Data Sources

 Security devices

 Servers and mainframes

 Network and virtual activity

 Data activity

 Application activity

 Configuration information

 Vulnerabilities and threats

 Users and identities

 Global threat intelligence

## Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents of the box

*Embedded Intelligence*

**Prioritized Incidents**

*Suspected Incidents*



# 安全运维平台和安全事件响应平台的集成

现状:

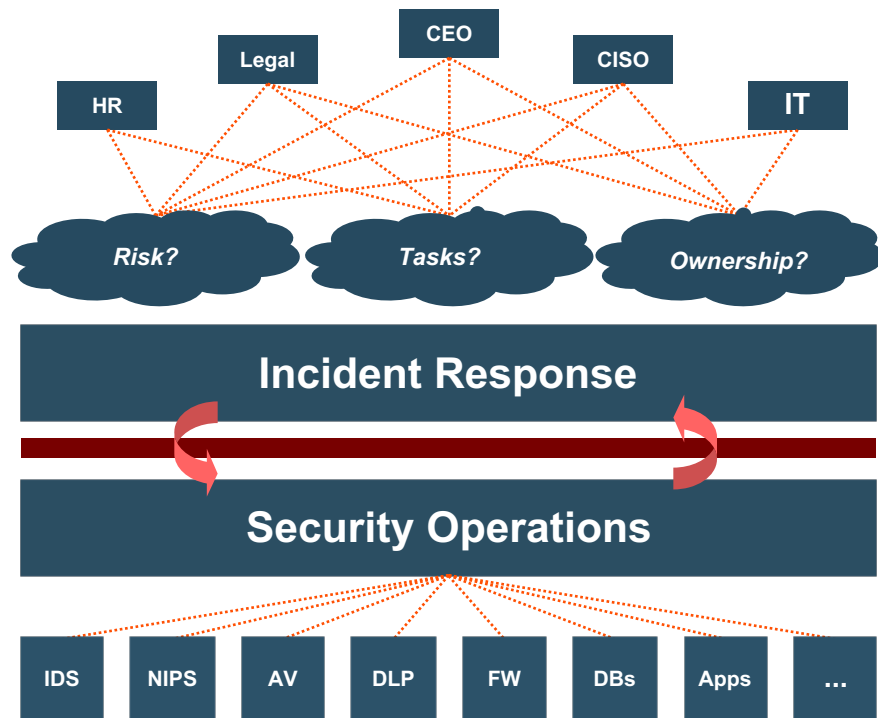
响应是手动的, 没有与安全运维平台集成

没有定制的相应流程

没有稳固的安全团队和工具

不了解安全条例

缺少专业技能



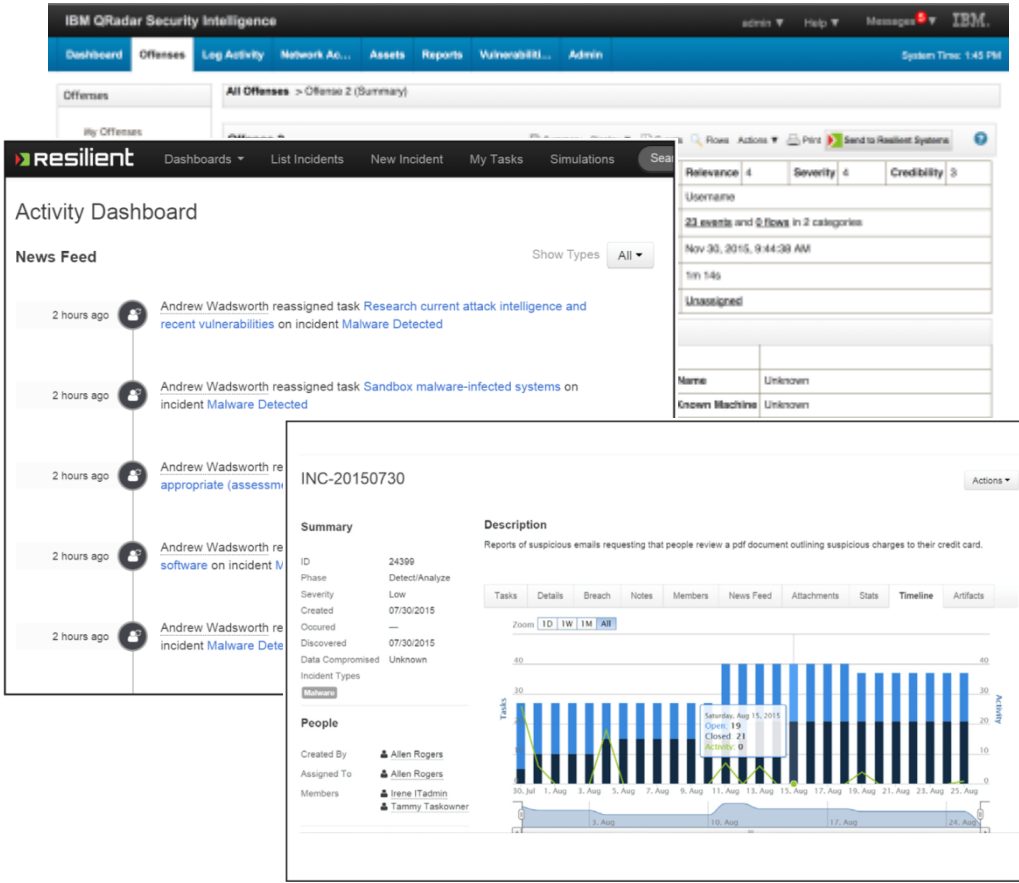
# QRadar 和 Resilient 集成

## 提供威胁检测和响应的单一平台

- 在Resilient 和Qradar之间安全事件无缝的自动和手动关联
- 将Qradar中的证据和Resilient中的案子相关联
- 事件的说明和状态自动同步

## 优点

- 缩短平均解决时间
- 确保一致性
- 符合监管要求和法律法规
- 更有效的利用员工执行耗时任务
- 提供事件响应流程的业务洞察和分析



# Resilient Systems和Qradar让安全团队在一个联合的安全运维和安全事件响应平台上协同工作



## 联合的安全运维和安全事件响应

*Resilient Systems will extend IBM's offerings to create one of the industry's most complete solutions to prevent, detect, and respond to threats*

## 为安全事件响应管理提供单一平台

*Resilient Systems will allow security teams to orchestrate response processes and resolve incidents faster, more effectively, and more intelligently*

## 与IBM和其他第三方解决方案无缝集成

*Resilient Systems integrates with QRadar and other IBM and 3rd party solutions so organizations of various sizes can successfully resolve attacks*

# IBM把Qradar打造成SOC安全运维平台的核心

- 2016 2Q 收购Resilient 安全响应平台
- Watson for Cyber security
- UBA(用户行为分析)
- X-force exchange
- App exchange



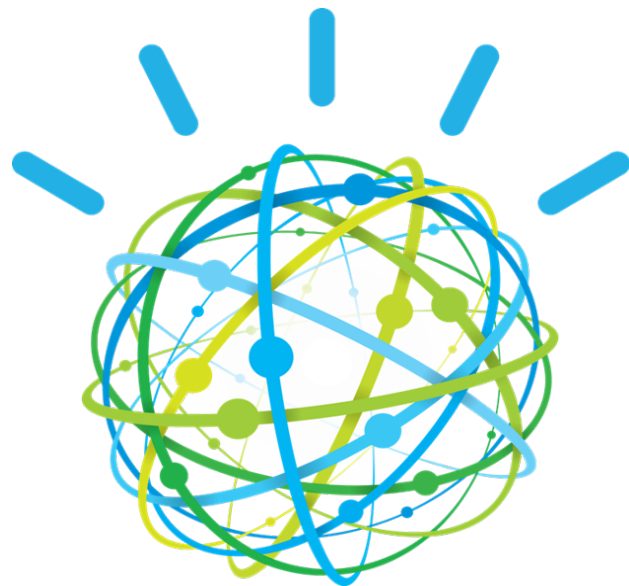
# 认知安全

# 认知：介绍… IBM Watson 网络安全

变革怎样进行安全分析工作

## 开启新的可能性.

世界上第一个采用Watson技术的认知分析解决方案来帮助分析理解，找出原因，并了解安全议题和威胁。



# 大量的安全数据被创建，但其中大部分却未被使用

传统安全数据

- 安全事件和告警
- 日志和配置数据
- 用户和网络行为
- 威胁和脆弱性信息的输入

人类产生的知识

## 大量的安全知识未被用来防御

通常企业之利用了其中内容的8%左右

例如:

- 研究文献
- 行业出版物
- 取证信息
- 威胁情报注释
- 会议演讲
- 分析报告
- 网页
- Wikis
- 博客
- 新闻来源
- 简讯
- 微博



# 安全性在历史上的三个时代



**外围控制：  
限制型安全。**

2005 年之前

它通过限制访问来确保数据安全，但随着黑客找到替代方法，这种方式开始无效。

**安全情报：  
启发型安全。**

2005+

其中包括实时监控数据的访问方式及访问者。然后利用分析检测偏差，帮助安全专家首先解决最大的问题。

**认知安全：具有理解、推理和学习能力的  
安全。**

2015+

安全情报已不足以满足需求，因为它只能识别和优先处理已知的威胁，而无法应对新出现的威胁。认知安全通过理解 80% 非结构化数据弥补了这种不足，这些非结构化数据存在于数以千计的研究报告、会议材料、学术论文、新闻报道、博客文章、行业警报等之中。

# 5 use cases:

## 释放认知

- 
- 1.提升 SOC 分析师的工作效率。**认知安全快速、大量处理结构化和非结构化数据，让分析师有时间提出见解。
  - 2.借助外部情报快速反应。**认知安全可帮助您在尚未出现威胁迹象时即可知晓威胁。
  - 3.借助高级分析识别威胁。**快速检测存在风险的用户行为、数据外泄和恶意软件，从而防患于未然。
  - 4.加强应用程序安全性。**认知安全可以将数以千计的漏洞分析结果提炼成一组少量的可操作项目，并且跳转到代码中可以修复漏洞的位置。
  - 5.降低企业风险。**认知系统可使用自然语言处理功能来查找敏感数据并对其进行编辑。

# 认知：彻底改变分析师的工作方式

## 理解并学习安全方面的自然语言

The screenshot displays the IBM QRadar Security Intelligence interface. The main view shows a network diagram for an offense (8324). A central node labeled 'Locky' (marked with a red 'A') is connected to several other nodes, including 'scorpena.com/665f46vb.exe', 'dw20.exe', 'yearend.xls', and '178.212.255.32'. A blue callout box above the diagram states: "QRadar has determined malware family or campaign may be related to the offense and 3 other hosts in your networks appear to be affected. QRadar has also found these additional indicators possibly related to the incident containing 14 Domains, 130 IP Addresses, 7 Geographies, 8 file HASHes".

On the right, a Watson Insights panel for Incident 8324, titled "Suspicious Action from Document", provides a summary of findings:

- Attack Campaigns: 1 (Locky)
- Documents Found: 42
- Domains Implicated: 14
- Hosts Involved: 4

The panel also includes a "Watson Insights" section with the text: "QRadar has determined malware family or campaign may be related to the offense and 3 other hosts in your networks appear to be affected. QRadar has also found these additional indicators possibly related to the incident containing 14 Domains, 130 IP Addresses, 7 Geographies, 8 file HASHes".

Below the diagram, a blue box contains the text: "Watson determines the specific campaign (Locky), discovers more infected endpoints, and sends results to the incident response team".



# IBM X-force Exchange

安全团队使用多种情报来源来辨明网络威胁，但这也带来了新的挑战

65%

利用外部威胁情报，以提高他们的安全决策<sup>1</sup>

然而，安全团队缺乏关键支持，以最大的使用这些资源

分析师无法从噪音中分离有用信息



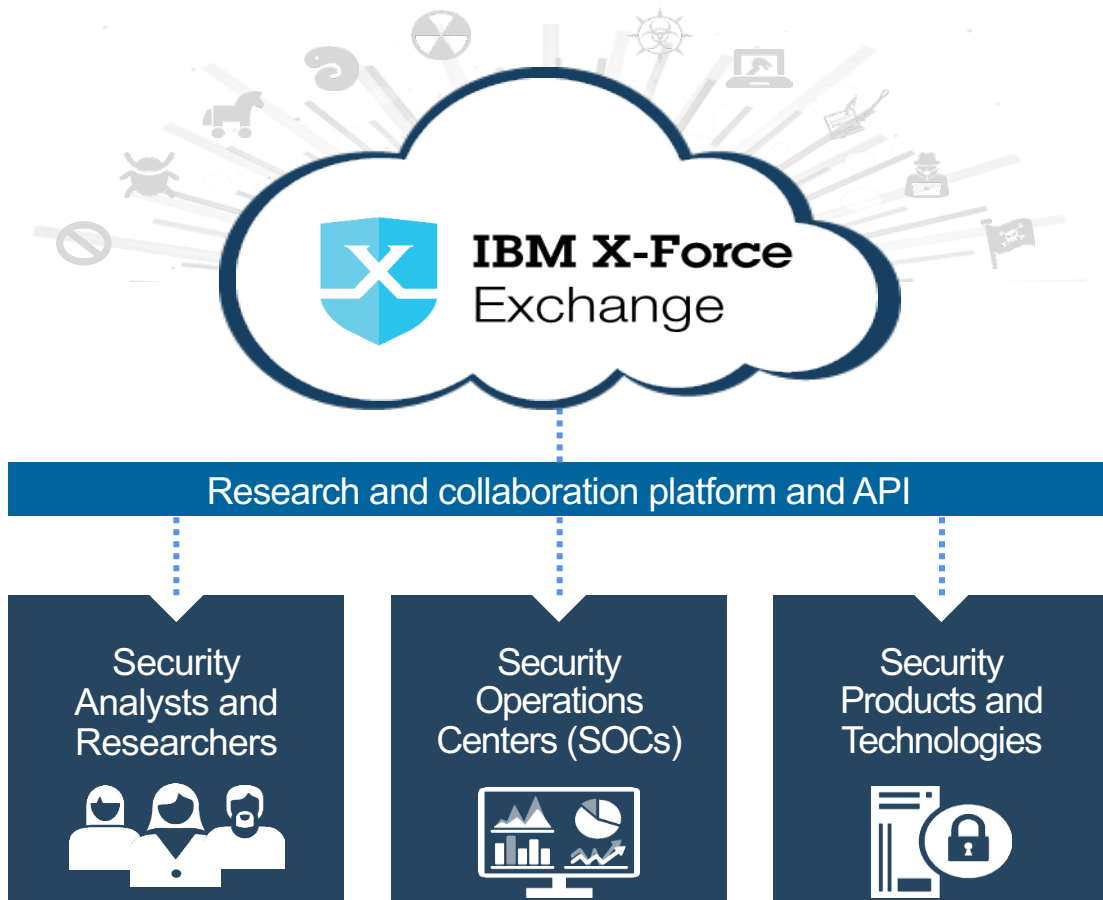
数据收集于不可信来源



需要很长时间将信息变得可操作



# 一个使用,分享,并依此智能情报来行动的新平台IBM X-Force Exchange



## 开放的

一个强大的平台，拥有丰富的威胁情报数据

## 可操作

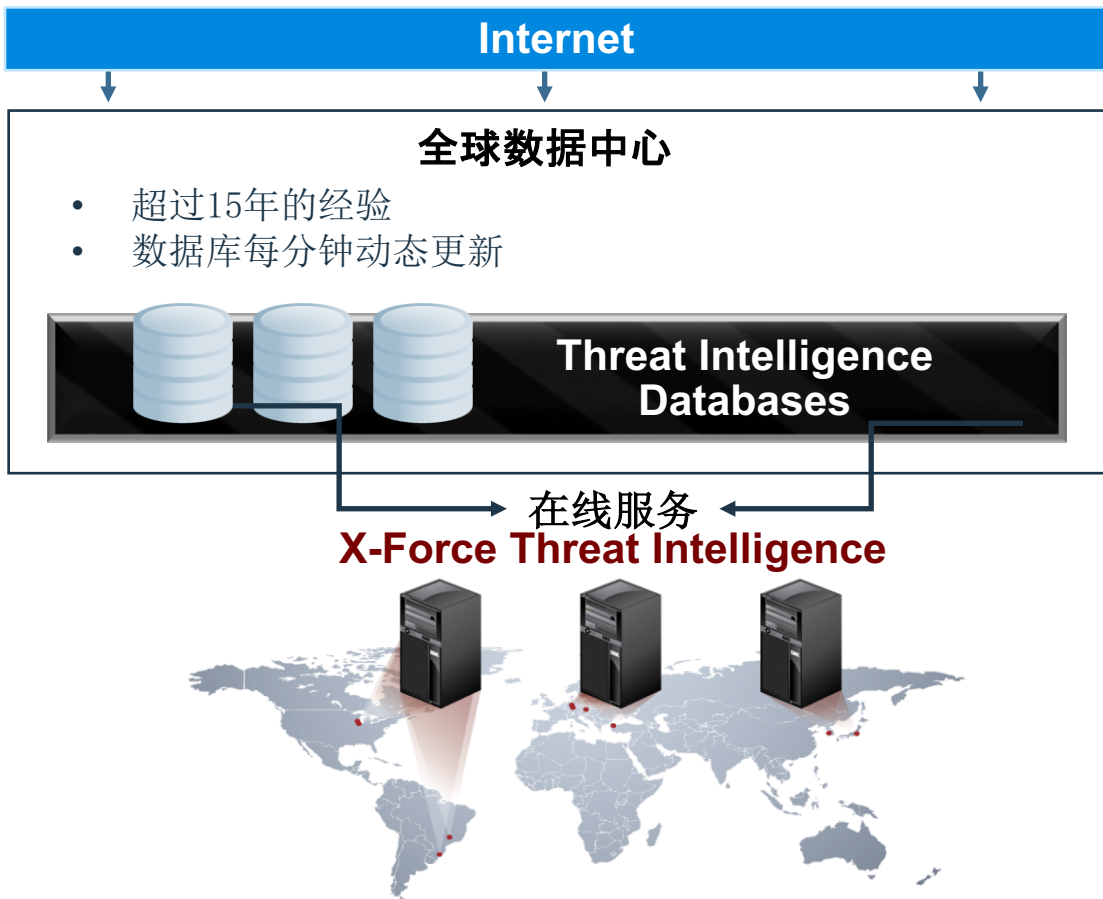
一个集成的解决方案，以帮助快速阻止威胁（STIX/TAXII，API）

## 社交的

共享威胁情报的协作平台

由IBM X-Force的声誉和规模为后盾

## IBM X-Force Exchange利用了来自IBM安全的大量情报信息



- 每天监控超过15B+ 的安全事件来获取匿名威胁信息
- 从270M+终端实时获取全球威胁情报
- 监控25B+网页和图片获取威胁数据
- 超过100K+个漏洞的世界最大数据库之一
- 基于8M+的垃圾邮件和网络钓鱼攻击深度情报分析
- 860K+的恶意IP地址信誉数据

# 共享威胁情报的协作平台

发现新的恶意软件域，  
并将其在X-Force  
Exchange标记

事件响应



1

安全分析师



2

查找此域并应用阻断规则以快  
速阻止恶意流量。并通过  
Exchange与CISO分享此信息



IBM X-Force  
Exchange



3

CISO

将此域添加到公共收藏  
夹并命名为“针对金融  
行业的恶意流量来源”  
并将此与业内同行分享

通过对等协作对威胁增添上下文

- 连接业内同行以验证结果
- 分享IOC (Indicators of Compromise) 指标以协助调查取证

IBM  
X-FORCE

这是第一次，客户可以直  
接与IBM X-Force安全研究  
人员和专家交流





# IBM Security App Exchange

# IBM Security App Exchange

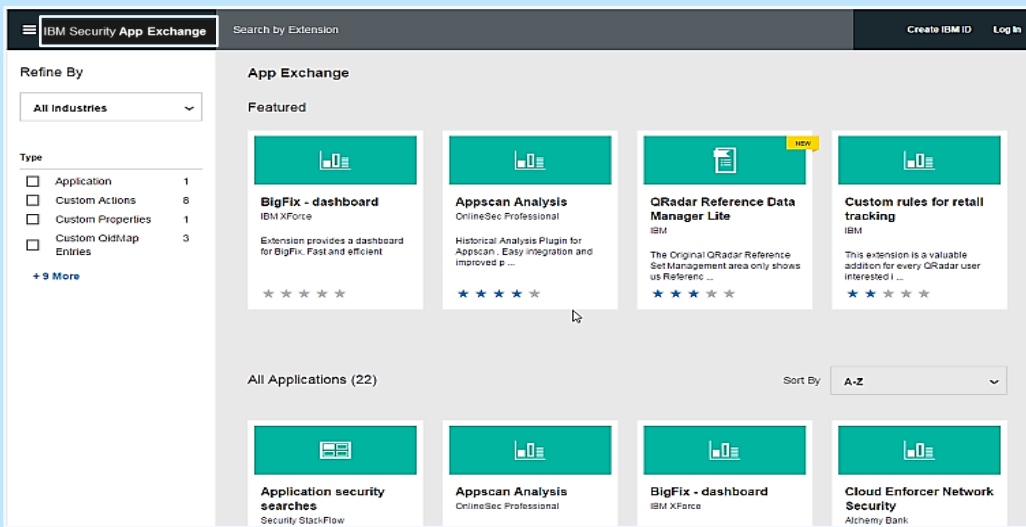
安全智能合作的新平台

简化认证的安全应用

单一协作平台

连接合作伙伴创新

快速扩展QRadar功能



为IBM安全解决方案快速提供新应用程序和内容的协作平台

允许Qradar用户和合作伙伴以更快的方式部署新的使用案例

## IBM | 威胁情报应用 (Threat Intelligence App)

- 通过开放的STIX/TAXII格式获取威胁情报
  - 在QRadar引用集 (Reference sets) 中加载威胁指标
  - 使用引用集 (Reference sets) 来关联, 搜索, 生成报告
  - 创建定制规则以做出响应
- 使用案例:  
将从XFE公共收集的IP地址生成监视列表, 并创建一个规则, 当攻击中包含列表中的IP时, 提升其严重性



The screenshot displays the Threat Intelligence App interface. At the top, there are buttons for "Add Threat Feed" and "Create Rule Action". Below this, the "Configured Threat Intelligence Feeds" section shows a feed configuration for "https://api.xforce.ibmcloud.com/taxii". The feed details include "Collection: xfe.collections.public" and "Reference Set: Web Servers". A downward arrow icon indicates "Signatures received last".

An overlay modal window is shown, titled "Enter credentials to connect to the TAXII server, then click the 'Discover' button to choose a collection to poll." The modal contains the following fields:

- TAXII Endpoint**:
- Authentication Method**:
- Username**:
- Password**:
- Discover**:
- Collection**:
- Action Name**:
- Properties**:
- Observable Type**:
- Indicator Type**:
- Cancel**:
- Add Action**:



## IBM | 安全事件概览 (Incident Overview App)

- 在Qradar上可视化所有的安全事件（攻击）
- 气泡的颜色和尺寸表明了安全事件的强度
- 在攻击气泡图中包含的IP之间的联系表明了共享IP地址
- 快速辨明威胁的严重程度和整体影响  
点击气泡让你一览无余的看到事件的细节
- 通过理解数据流实现更快的响应
- 理解攻击链



# 合作伙伴应用 – Carbon Black/Bit9

## IBM | Carbon Black App for IBM QRadar



在QRadar界面中显示终端的完整视图并可对攻击做出响应。

- 在QRadar控制台中嵌入终端的信息
- 检测并对终端活动采取行动

- 仪表盘显示了Carbon Black集群的基本信息和状态（传感器数量，健康状况，可用磁盘空间等等）
- 颜色将基于状态发生改变（绿色，黄色，红色）。

The image displays three overlapping screenshots of the IBM QRadar Security Intelligence and Carbon Black interfaces. The top screenshot shows the QRadar dashboard with tabs for Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Vulnerabilities, Admin, and CarbonBlack. The middle screenshot shows the Carbon Black interface with a search bar and options for Sensor Status and Watchlist Hits. The bottom screenshot shows a detailed view of processes with a table listing process names, groups, hostnames, and parent processes, along with charts for Host Type, Hour of Day, Day of Week, and Process Start Time.

# AppExchange 目前包含超过几十个应用插件

<http://apps.xforce.ibmcloud.com>

优化依据

所有行业

类型


- 应用程序 7
- 定制属性 16
- 定制 QID 映射条目 1
- 定制规则 7
- 仪表盘 1
- FGroup 7
- FGroup 类型 7
- 其他 1
- 参考数据收集 6
- 报告 3
- 保存的搜索 4

## Welcome to the Security App Exchange

# Find. Download. Use.

Verified extensions for a stronger enterprise defense.

### 特色




#### 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 ...

★★★★★



# THANK YOU

## FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. 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.

**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.