IBM Security

以威胁情报和人工智能为趋动的 QRADAR现代安全运营中心

黄俊华
IBM 大中华区 QRadar & Resilient 业务经理
18610455566, bjjhhjh@cn.ibm.com

April 1, 2019

IBM

IBM Security：简介

关于我们

- 全球**最大的**企业网络安全提供商
- **17,500 多**家客户
- **133** 个国家/地区
- **3,500 多**项安全领域专利
- **20** 次安全领域企业并购（自 2002 年）
- **6000** 多名研发与咨询专家

X-Force Command Center

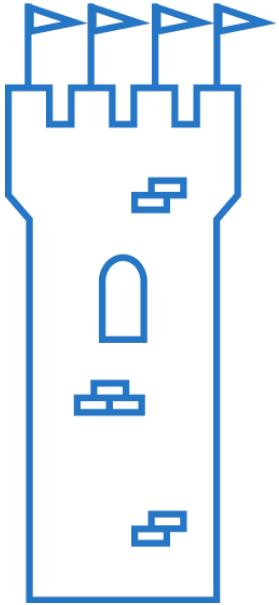
- 每月监控超过 1 万亿次事件，每天提供 200,000 多条威胁情报
- 在全球设有 9 家办事处

领导者 - 安全市场所有 12 个细分领域的领导者

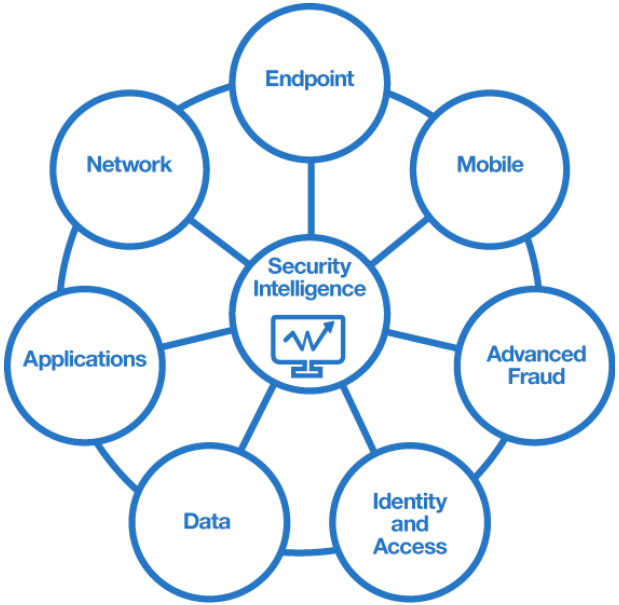
领域	细分领域	分析机构的评估结果
安全运营与响应	安全智能	领导者
	网络保护	领导者
信息风险与保护	身份治理与访问管理	领导者
		领导者
		领导者
		领导者
	数据安全	领导者
	应用安全	领导者
	终端保护	领导者
	欺诈防范	领导者
安全转型服务	咨询与托管服务	领导者
		领导者

IBM安全全球布局概览

信息安全的时代演进



战壕，城堡



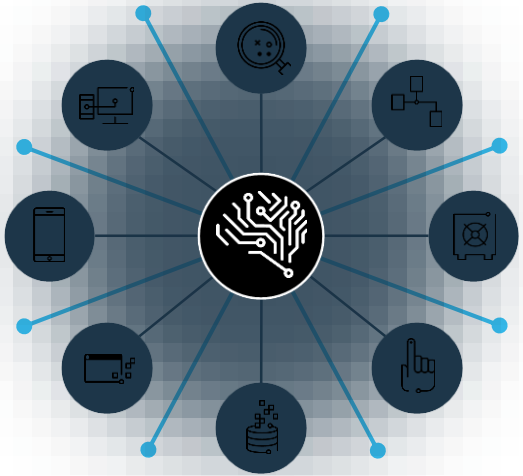
智能，集成

云，认知

面对海量的安全数据，安全人员需要从多个角度印证安全事件的严重程度和可信度

场景

1. 主机访问恶意IP地址，但这类问题每天会数以千计；
2. 这个恶意IP地址在过去的几天曾经针对该主机运行的服务进行漏洞利用；同样，这类问题也很寻常；安全人员需要确定该主机的重要性，不清楚漏洞利用是否成功，也不清楚该主机是否存在相应的漏洞；
3. 通过观察网络流量，该IP地址已经与内部主机建立了大量连接；



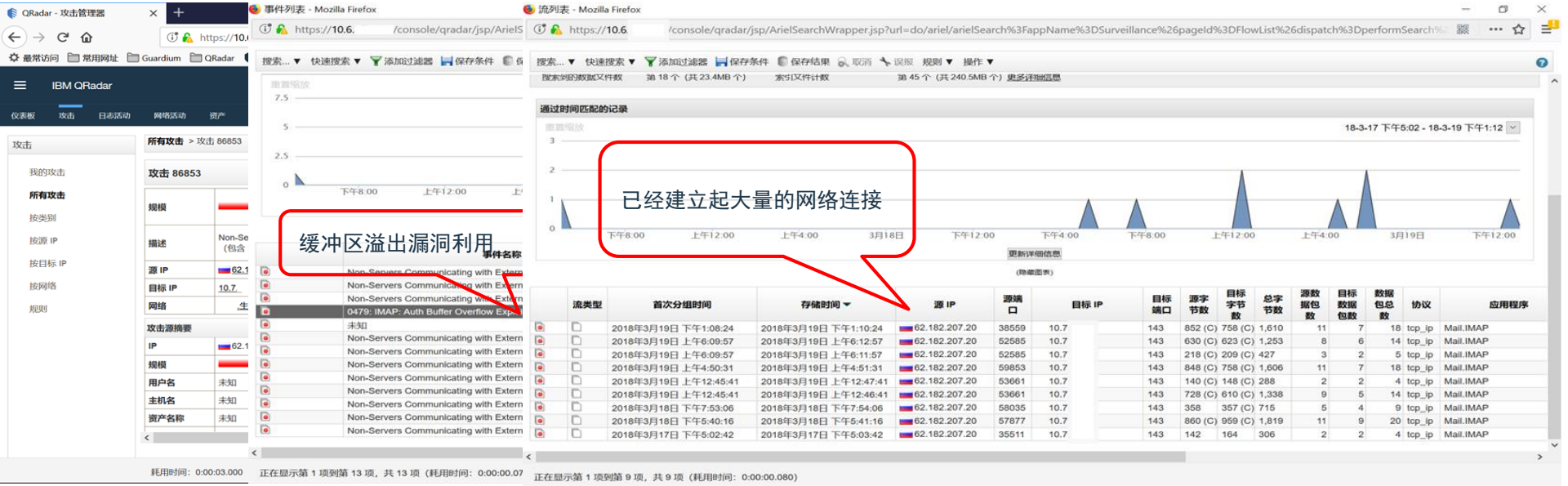
安全态势感知系统可以将此三个条件进行归并形成成一个单一的高危警报

平台能力

日志分析 | **网络流量分析** | **威胁情报** | **关联分析**

场景举例 – 如何将日志、流和威胁情报信息结合，关联化发现问题

- 场景描述：
  - QRadar报出攻击，指明邮件服务器与外部动态IP（*信息来自于X-Force威胁情报*）地址有通讯活动；
  - 在相关事件中，发现该动态IP地址有针对邮件服务器进行缓冲区溢出的漏洞利用（*信息来自于IDS*）；
  - 在相关的网络流量中，发现该动态IP地址已经与邮件服务器的143端口有大量的通讯连接（*信息来自于网络流量*）；



检测并制止威胁

IBM QRadar

用户与实体分析
统计分析
范例识别
实体和用户情境
基于网络的异常检测
外部威胁关联
实时分析
基于风险的分析
威胁捕获
DNS 分析
业务情境

在高级威胁防御 SIEM 领域位列第一

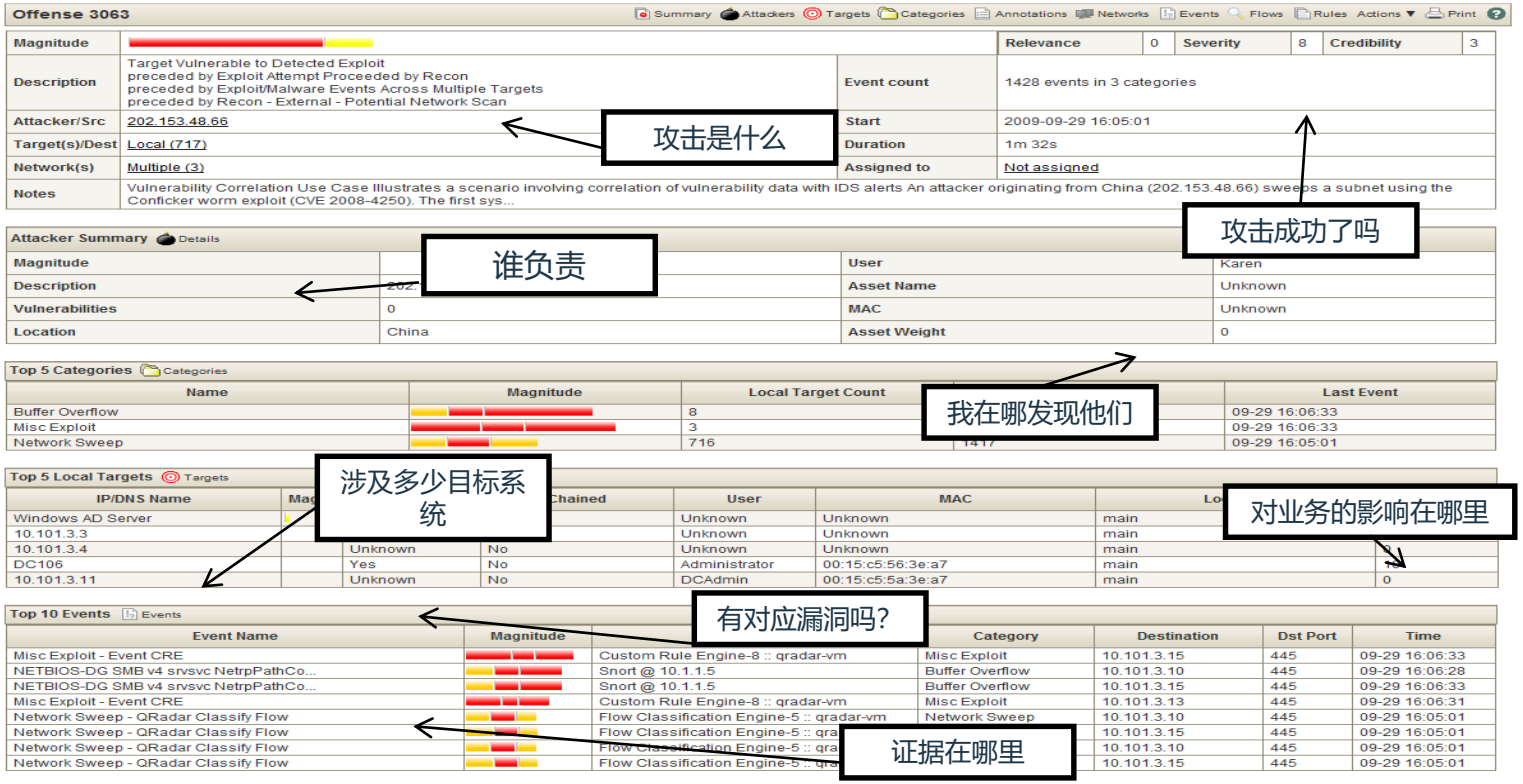
- Gartner

“每天可准确分析 30 亿次安全事件，然后将其汇总为 25 次需优先处理的攻击，让分析师专注于最重要的事情。”

- 某家大型能源公司

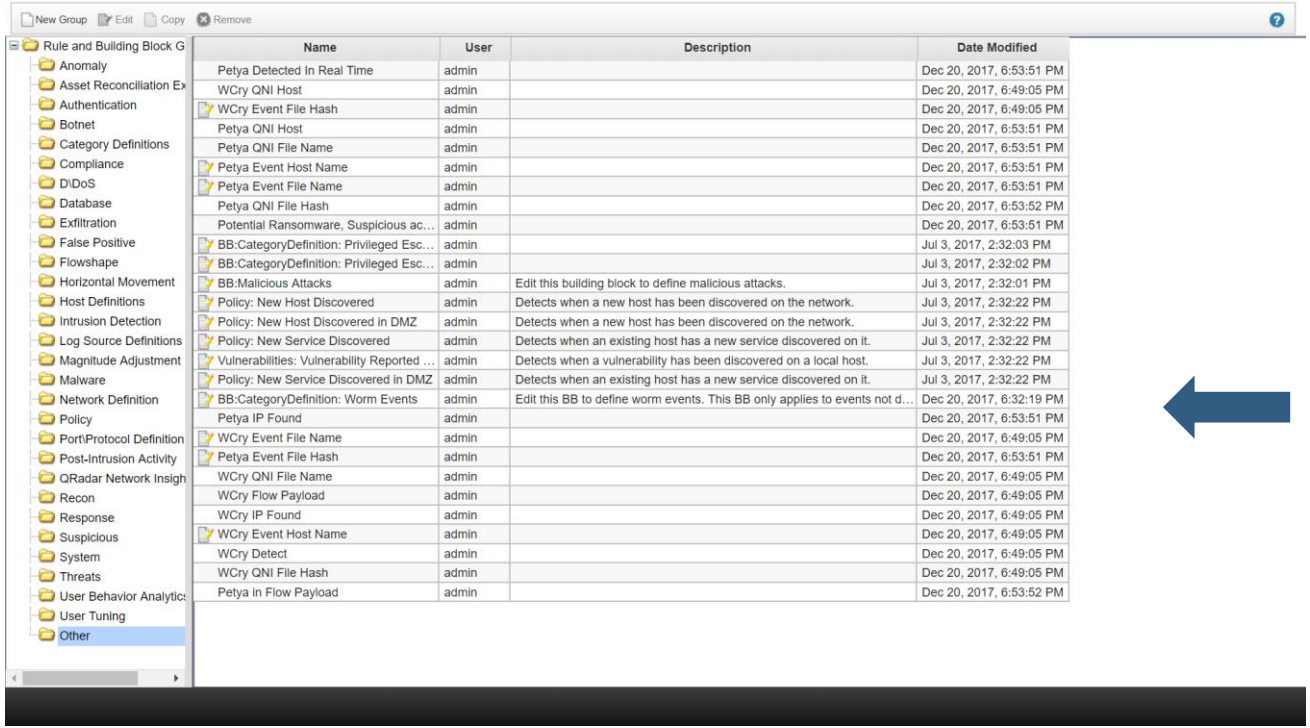
发现潜在的攻击行为

清晰、准确、全面的提供相关信息



关联分析 – 18大类，600多种开箱即用的规则

- QRadar提供了非常强大的关联分析、异常检测、用户行为分析、实时深度包检测等功能，威胁分析和检测的能力和范围非常广。



QRadar内置的规则集

将网络分析更进一步

QRadar事件取证和网络数据包捕获（QRadar Incident Forensics and Network Packet Capture） 可以捕获，重建并回放整个会话

事件响应

事件侦察

QRadar 网络洞察（ QRadar Network Insights） 也会让你发现，在会话中任何时候是否有可疑主题或你关注的主题

QFlow 提供网络流分析的所有优势，可以识别7层流中的应用程序，并可以捕获进程的包头。

“ 网络流量 实质上是网络上两个主机之间的对话记录……这个信息很像电话账单：你不能说出谈话中所说的话，但你可以用它来证明谁和谁说话”。
- SANS Institute

由数百个开放集成提供支持

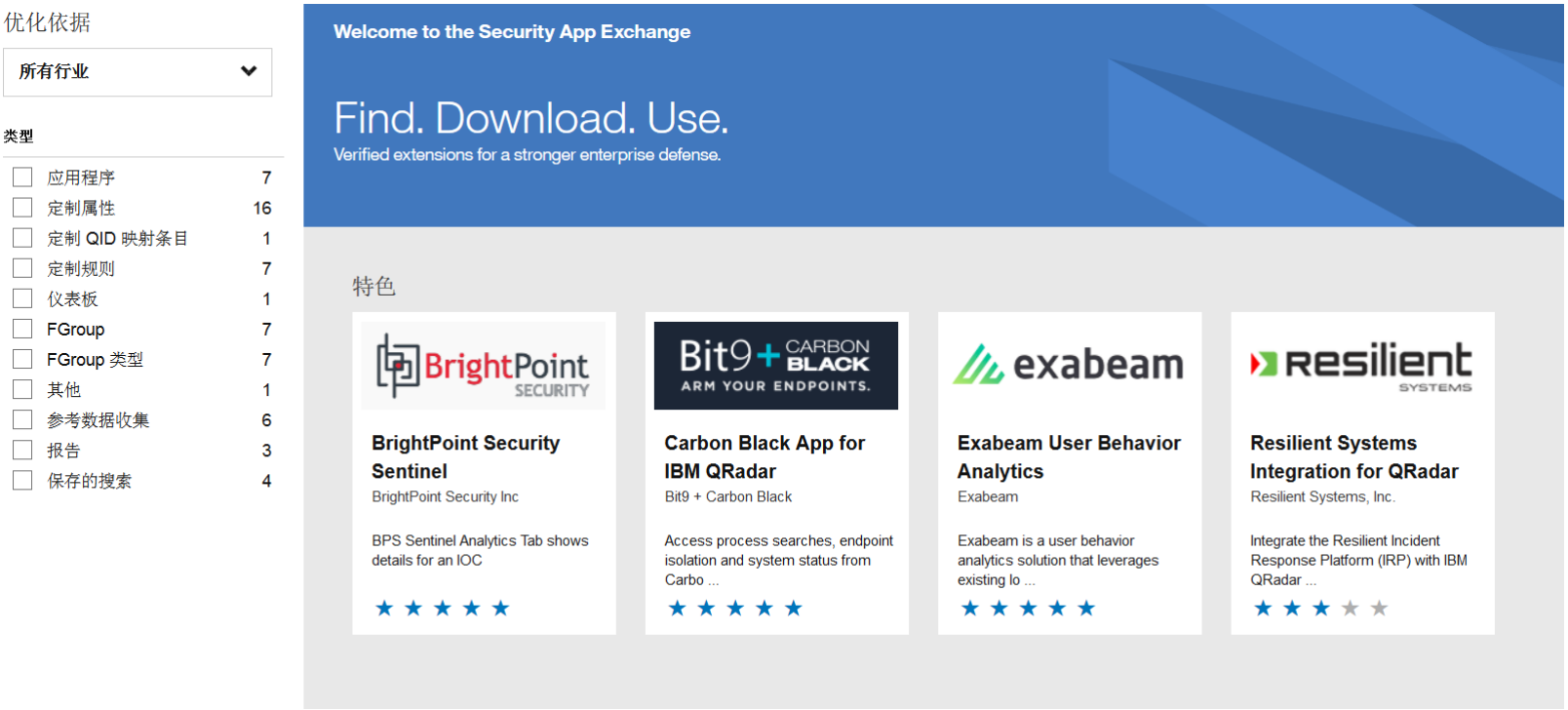
IBM QRadar 广泛第三方产品，包括国产设备和系统

IBM QRadar
Security Intelligence Platform

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

SHARED UNDER NDA UNTIL MAY

可扩展性 – AppExchenge目前包含超过170应用插件



“人工智能”和“统筹”加速安全运维的智能和自动化水平

交付智能的安全运营中心

威胁管理

快速、自信地识别和响应威胁

若要做到这一点，我们需要将人员、流程及技术与 AI 及持续洞察力互联一体

我们面临着哪些妨碍因素？

- 躲避基于规则的解决方案的攻击者
- SOC 中的职位空缺和流失
- 事件数量过多、时间不够
- 无法实现响应的运营化
- 没有足够的人员来处理数据泄露

Security Operations Consulting | Threat Management Services | Security Analytics | Response and Orchestration | Threat Hunting

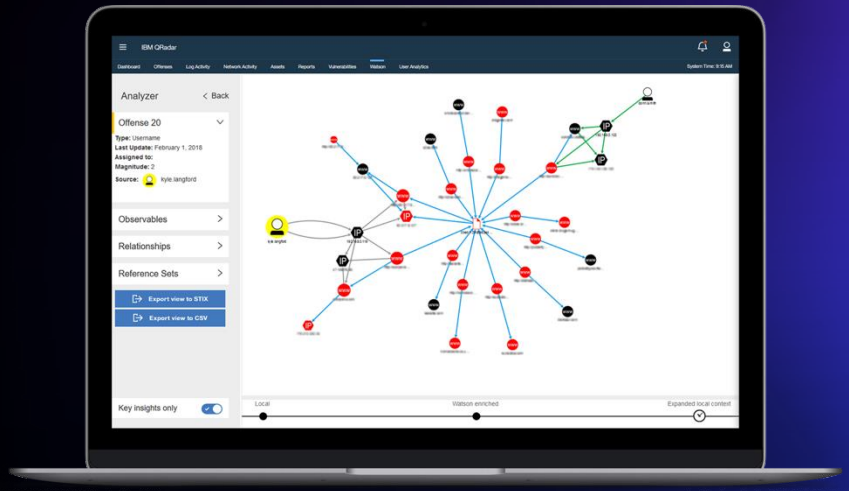
借助 AI 加速 SOC 运营

IBM QRadar User Behavior Analytics

通过机器学习检测内部人员威胁

- 持续学习行为，以预测恶意用户
- 为单个用户生成详细的风险评分
- X-Force App Exchange 上有 16,000 个应用可供您免费下载

IBM QRadar Advisor with Watson



借助 AI 提升团队的效率

- 自动“连点成线”，以便更明确地提交威胁
- 借助 MITRE ATT&CK 加快响应速度并实现攻击阶段的可视化
- 通过 Watson 的100 多亿个安全数据点获取洞察力

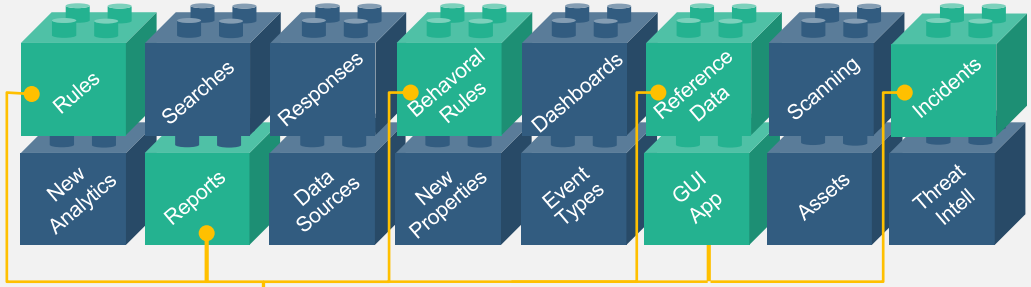
User Behaviour Analytic (UBA) :内部威胁

关心的一些问题:

- 通过钓鱼或恶意软件帐户导致的凭据被盗
- 凭据被滥用
- 客户数据和/或知识产权的窃取
- 用户是否正在执行使自己和组织面临更大风险的活动

Enabling greater flexibility and less complexity

QRadar API Components



Cybersecurity Use Cases

Insider Threats

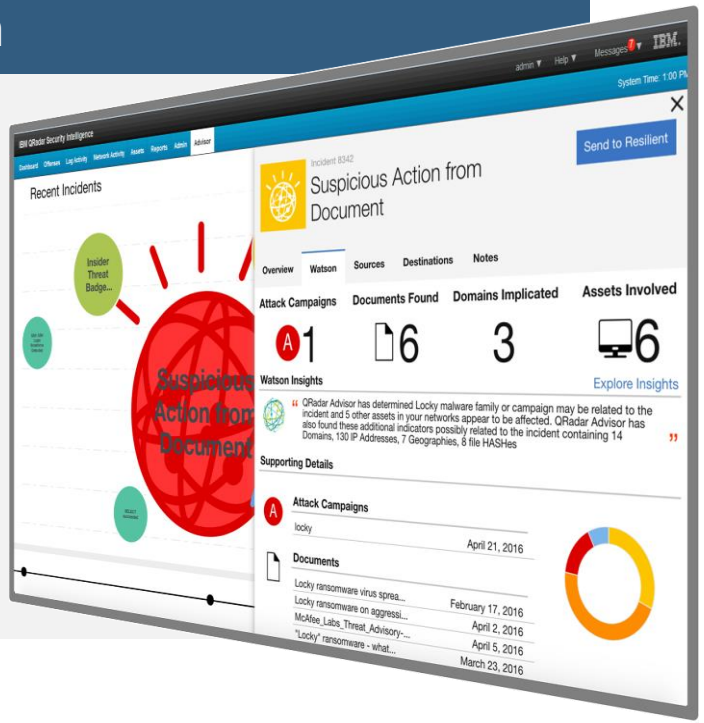
Internet of Things

Incident Response

认知安全开始的篇章
IBM Security 在安全运维领域，革命性的变革

全新! IBM QRadar Advisor with Watson

- 借助认知的能力，辅助安全分析师调查和验证安全事件和异常行为
- Watson for Cyber Security 使得海量的安全知识可以被学习和利用，针对特定的安全事件提供见解和洞察力
- 转变SOC运维模式，解决了当前棘手的挑战，诸如：技能短缺、过量的报警、事件响应延迟、 处理风险等
- 设计为简单易用：通过IBM Security App Exchange下载，分钟级完成部署



65% 的企业使用外部威胁情报来加强他们的安全决策

安全团队通常缺乏关键的支持来充分利用这些资源

分析师不能将有用的信息与繁杂的信息分开

情报的来源往往包含了未被检验的提供者

花费大量的时间来找出可做决策的信息

[1] Source: ESG Global

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

响应方式非常重要

IBM Resilient

使用业内领先的意外事件响应平台“武装”您的团队

40 倍

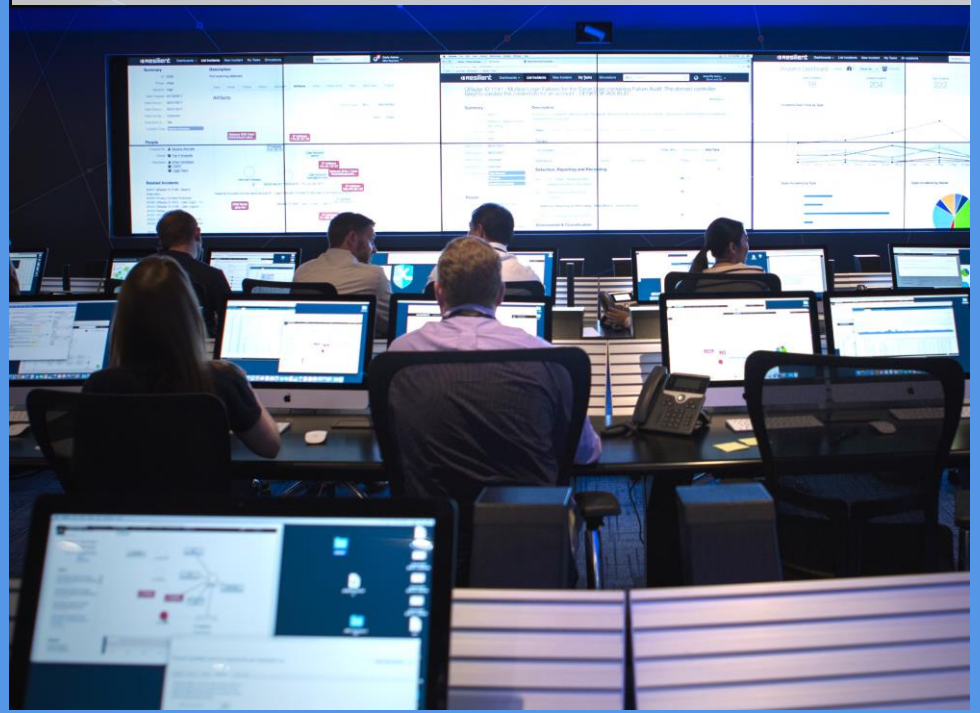
借助动态运行手册编排您的人员、流程和技术，可将整体响应速度提升 40 倍

IBM X-Force Command Center

在一个沉浸式的安全环境中测试

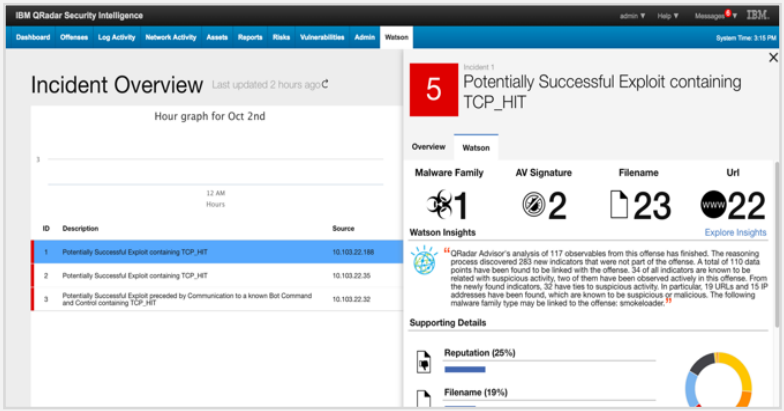
2,500 多名

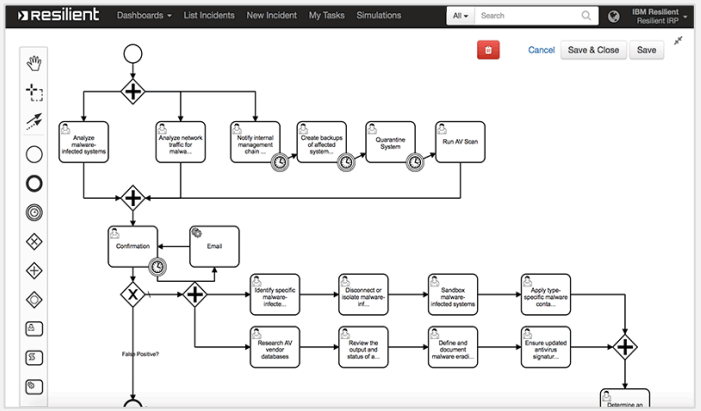
客户通过我们采用最新技术的沉浸式网络靶场接受了安全最佳实践方面的训练



安全运营的未来是AI与统筹（SOAR）

假使您能够增强团队的智能化水平和快速响应的能力？





使用AI 获得先机

自动化调查安全事件和异常，识别最可能的威胁

- 从海量的外部数据源中快速获得洞察
- 应用认知技术构建关联关系

IBM QRadar Advisor with Watson

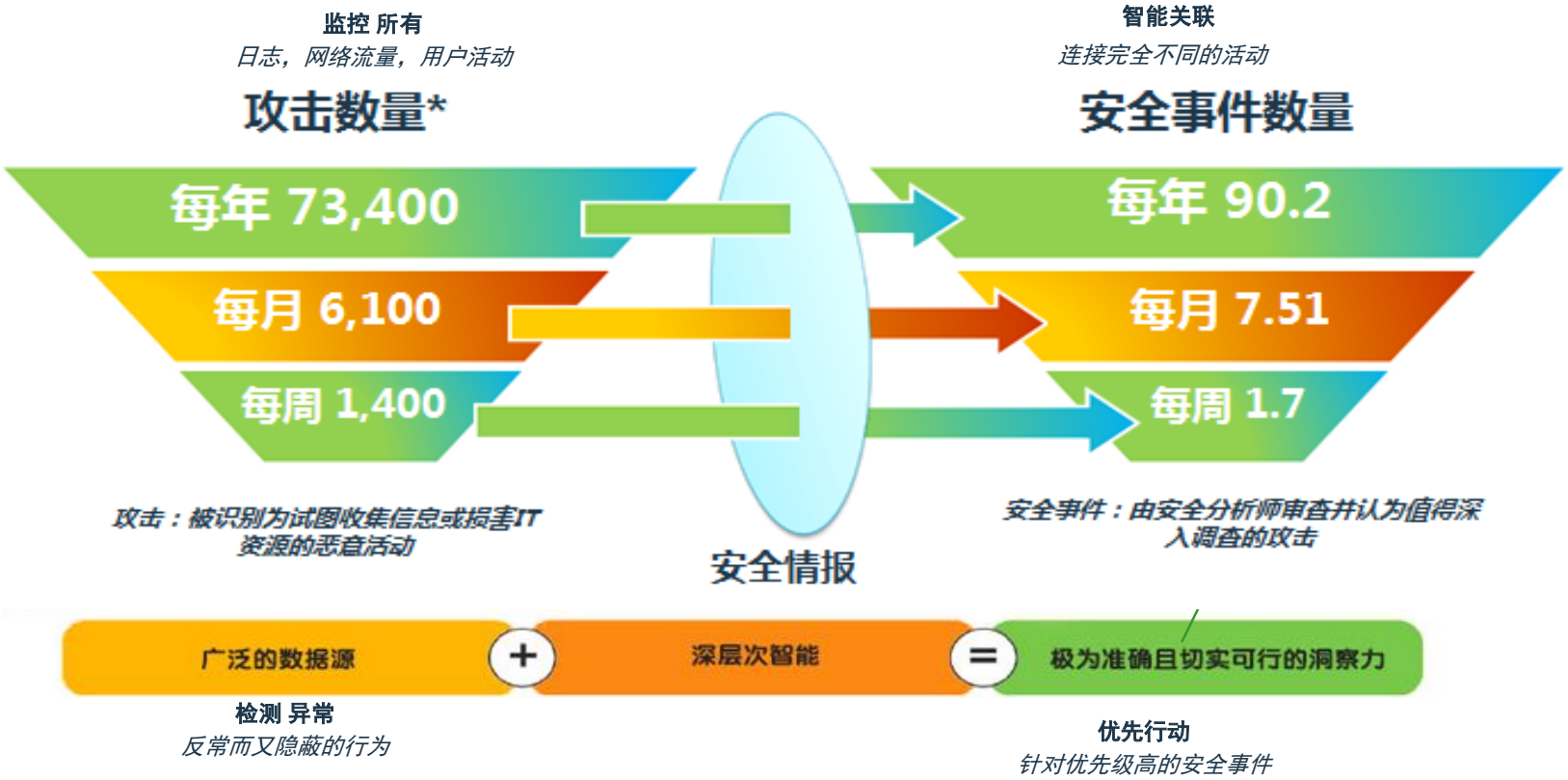
自如进行快速响应

统筹完整的和动态的响应，进行快速的更加智能的补救措施

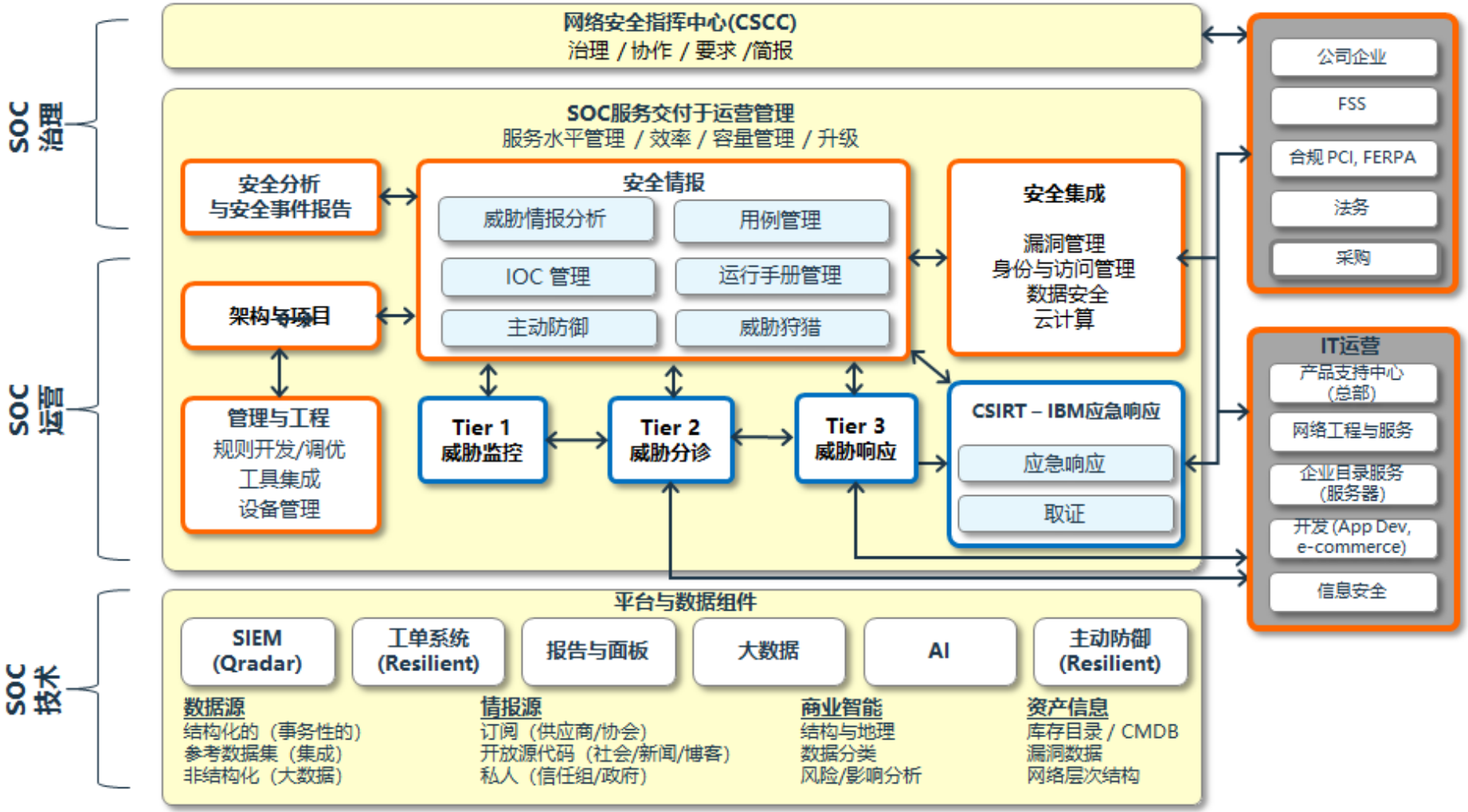
- 根据NIST / CERT / SANS创建动态的的操作手册
- 部署响应过程和专家技能

IBM Resilient

SOC平台极大提升了威胁检测和分析的效率



IBM SOC模型



IBM Security

THANK YOU

FOLLOW US ON:

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

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 ANYSYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

IBM